Structured approach to organisational ICT risk management: An empirical study in Thai businesses

A thesis submitted in fulfilment of the requirements for the degree of Doctor of Philosophy

SIRIDECH KUMSUPROM

B. Acc., M.B.A. (Dhurakij Pundit University)

MIS (Griffith University)

School of Business Information Technology and Logistics

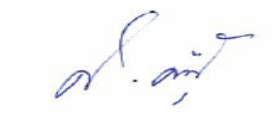
Business Portfolio

RMIT University

September 2010

Declaration

I certify that except where due acknowledgement has been made, the work is that of the author alone; the work has not been submitted previously, in whole or in part, to qualify for any other academic award; the content of the thesis is the result of work which has been carried out since the official commencement date of the approved research program; any editorial work, paid or unpaid, carried out by a third party is acknowledged; and ethics procedures and guidelines have been followed.



Siridech Kumsuprom

(Date 24/09/2010)

Acknowledgements

It is imperative to name the valuable people who have helped me throughout this long research journey. I am everlastingly appreciative for their contributions.

I would first of all like to express my deepest gratitude to my senior supervisor, Professor Brian Corbitt. His suggestions, comments and guidance have helped me through the research process and finally write this thesis. He has not only encouraged me to pass several critical phases but has also guided and enabled me to successfully complete this research.

I would also like to acknowledge my former senior supervisor, Professor Hepu Deng. His views encouraged me to start this research which importantly related to my educational background.

I am also indebted to Dr Siddhi Pittayachawan who assisted me with the quantitative data method and analysis using SEM. With his guidance and suggestions, I have improved my knowledge of statistical methods and techniques while analysing the quantitative data.

I would like to express my gratitude to the School of Business IT and Logistics, RMIT University and the Research Director, Professor Mohini Singh, who provided me with the approval for support funds to cover the expense of attending conferences and for the data collection phase in Thailand.

I would also like to express my appreciation to my second supervisor, Dr Leslie Young. His comments and suggestions allowed me to improve the quality of my writing.

I would like to express my gratitude to my former dean, Dr Pornsiri Punnakasem, who supported me by providing an idea to begin this research topic and also helped me to recruit participants for the interviews. My appreciation is also extended to Pannida Phairat and Saisuwat Phairat who helped me to recruit participants for the survey.

I would also like to express my indebtedness to my sponsor, Dhurakij Pundit University—including the president, the board of international scholarship and my current dean—who supported me not only with my tuition fees but also by providing me with a monthly allowance while studying and living in Australia.

I would like to thank Cherngchai Suwannakoot, Chin Eang Ong, Fu Mei Weng, Leon Kok Yang Teo, Kornkanok Duangpracha, Phoommhiphat Mingmalairaks, Smithtana Chaijenkij and all my PhD friends who have shared discussions with me about my research method, design and analysis, and helped me to improve the quality of my research. I would also like to thank Julia Farrell for her copyediting of this thesis.

Lastly, I am deeply grateful to my father Ananta Kumsuprom, my mother Apijit Kumsuprom, my brothers and my sister, who have always believed in my ability to complete this research and encouraged me even through the most difficult stages of my research.

Dedication

This thesis is sincerely dedicated to my family. Their love and encouragement have given me the support I needed to pursue this research.

(In Thai)

ปรัชญาดุษฎีนิพนธ์ (การจัดการสารสนเทศทางธุรกิจ) ฉบับนี้ ขอมอบให้แก่ครอบครัวของผู้เขียน ด้วยการสนับสนุนจากครอบครัวของผู้เขียนทั้งด้านความรัก ความเป็นห่วง และความเอาใจใส่ในทุกเรื่องช่วยให้ผู้เขียนสามารถได้มาซึ่งปรัชญาดุษฎีนิพนธ์ฉบับนี้

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AIRMIC	Association of Insurance and Risk Managers
AMOS	Analysis of Moment Structures
BSC	Balanced Score Card
CFA	Confirmatory Factor Analysis
CFI	Comparative Fit Index
CG	Corporate Governance
CLP	Corporate Level Plan
COBIT	Control Objectives for Information and related Technology
COSO	Committee of Sponsoring Organisations
EFA	Exploratory Factor Analysis
ELP	Enterprise Level Plan
ERM	Enterprise Risk Management
ESP	Enterprise Security Plan or Enterprise Information Security Plan
GOF	Goodness-Of-Fit
HRMP	Human Resource Management and Planning
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IFAC	International Federation of Accountants

IFI	Incremental Fit Index
IIA	Institute of Internal Auditors
IRM	Institute of Risk Management
IS	Information Security
ISACA	Information Systems Audit and Control Association
ISG	Information Security Governance
ISM	Information Security Management
ISO	International Organisation for Standardisation
ISO/IEC 17799	Information Technology–Security Techniques–code of practice for Information Security Management (ISO/IEC 17799:2005) in 01/07/2007 renumbered to ISO/IEC 27002:2005
ISO/IEC 38500	Corporate Governance of Information Technology Standard
IT	Management of ICT resources
ITG	Information Technology Governance
ITGI	Information Technology Governance Institute
ITIL	Information Technology Infrastructure Library
OGC	Office of Government Commerce
OLP	Operational Level Plan
OS	Organisational Security or Organisational Information Security
OSM	Organisational Security Management or Organisational Information Security Management
PCFI	Parsimonious Comparative Fit Index
POLICY	Organisational Policy
RMSEA	Root Mean Square Error of Approximation

SEM	Structural Equation Modelling
SICTRM	Successful Information and Communication Technology Risk Management
SPSS	Statistical Package for the Social Sciences
SRMR	Standardised Root Mean Square Residual
TLI	Tucker-Lewis Index

List of Publications

Kumsuprom, S, Corbitt, B, Pittayachawan, S, & Mingmalairaks, P 2010, 'Determinants of Successful ICT Risk Management in Thai Organisations', *PACIS 2010 Proceedings*, Taiwan, 9-10 July 2010.

Kumsuprom, S, Corbitt, B, & Pittayachawan, S 2008, 'ICT risk management in organizations: Case studies in Thai Business', *ACIS 2008 Proceedings*, Christchurch, 3-5 December 2008.

Kumsuprom, S, Corbitt, B, & Deng, H 2007, 'An integrated approach to organisational ICT risk management', *Proceedings of the 8th International Conference on Operations and Quantitative Management*, Bangkok, 17-20 October 2007.

STRUCTURED APPROACH to ORGANISATIONAL ICT RISK MANAGEMENT: AN EMPIRICAL ANALYSIS IN THAI BUSINESSES

Abstract

Risk management in relation to information and communication technologies (ICT) has become an essential means of organisational governance. In spite of the development of ICT risk management methodologies that have been published as numerous techniques and tools aimed at assisting organisations to deal with ICT risks, questions remain about the success of its methodology.

The Control Objectives for Information and related Technology (COBIT) framework is representative of this kind of risk management approach to addressing ICT risk management. It takes a holistic view of the organisation (Lainhart 2001a) and focuses on a top-down strategy which is used to describe the business functions, processes and tasks to support senior management developing, implementing and maintaining ICT governance across the organisation (Robinson 2005; Solms 2005a). Adopting a top-down strategy to manage ICT risks in an organisation means that the organisation is concerned more with whole-of-business view than with technical solutions to ICT risk management. As a result the emphasis is on organisational structure and content (Solms 2005b). Existing research, however, shows that organisations appear to lack the required technical sophistication in their internal audit management when using this top-down approach (Viator & Curtis 1998; Hermanson et al. 2000). Clearly, delineate technical orientation and business orientation are part of the planning for effective ICT risk management.

In order to address this issue, a bottom-up approach to ICT risk management has also been developed and its impact reported in the literature (Solms 2005a). One representative of this bottom-up approach is the ISO/IEC 17799 (renumbered ISO/IEC 27002 in July 2007) standard for effective ICT risk management (Martinez et al 2010). The ISO/IEC 17799 standard is an information security governance framework which focuses on a detailed technical or bottom-up approach (Saint-Germain 2005; Solms 2005a). A bottom-up approach emphasises technical security and elaborates on all processes dealing with ICT risk in detail. It also provides an organisation with general guidelines on how the ISO/IEC 17799 standard can be utilised to control, prevent and mitigate ICT risks.

This research addressed the question "What factors determine successful ICT risk management in a business organisations in the Thai business context?", and three subsidiary questions "What are the current profiles of ICT risk management in Thai organisations?"; "How are ICT risk management concepts applied in those Thai business organisations?" and "What are success factors can be identified for successful ICT risk management derived from the adoption the COBIT framework and the ISO/IEC 17799 standard?". The COBIT framework and the ISO/IEC 17799 standard are used extensively to define organisational governance of business; and ICT and security functions, processes and tasks to help management develop and implement strategies and policies for effective ICT risk management. This research explores the understanding of ICT risk management in Thai business context.

A mixed-method research approach was used to explore ICT risk management in a selection of Thai organisations. The findings from six case studies indicate that successful ICT risk management results from collaboration between management level activities and operational level activities. The adoption of the COBIT framework and the ISO/IEC 17799 standard in the case study companies revealed that success was dependent on six key factors: the creation of organisational policy, the management of people and their behaviour in organisations, the management of organisational ICT security, the management of ICT resources, the corporate level plan and the operational level plan. To confirm the outcomes of the case study research a survey was developed and administered to over 50 Thai organisations and across three types of industry (Banking, Technology and Insurance) listed on the Stock Exchange of Thailand. The data was analysed using structural equation modelling (SEM). The findings of the analysis of the survey data showed that there were three main factors—the effective creation of organisational policy, the effective management of ICT resources, and the effective planning of enterprise information security that drive successful ICT risk management in the Thai organisations surveyed.

This research sought to investigate the current profile of ICT risk management to identify and then model the success elements of ICT risk management in a sample of Thai business organisations. This research supported and confirmed previous research that argues that policy must be structured, first at the board of directors and then at the levels of senior management and operational management, who together must delineate the procedures and practices for dealing with ICT risk management. In dealing with ICT risks, several frameworks and standards have been introduced but ICT risks still persist, therefore, the implication of this research was that we can learn from the Thai organisations that organisations needed to consider the success factors when managing ICT risk. This research proposed that three main success factors affect ICT risk management in Thai organisations. Firstly, the effective organisational policy helped the

Thai organisations to plan the effective management of ICT resources and the effective planning of enterprise information security. Secondly, the effective management of ICT resources facilitated the planning of enterprise information security to achieve successful ICT risk management planning. In addition, the survey results have shown that effective organisational policy was the main influence on the management of ICT resources and the planning of enterprise information security. All three success factors complement each other and were significant together in terms of strategic development (i.e. policy) and strategic implementation (i.e. management direction). Lastly, the effective planning of enterprise information security was shown to be a critical factor that helped an organisation mitigate, prevent and avoid operational, technical and strategic risks related to ICT. All three success factors were initially drawn from both the COBIT framework and the ISO/IEC 17799 standard and were found to positively contribute to successful ICT risk management.

Chapter 1
INTRODUCTION

This thesis is based on a study of the use of standards in ICT risk management in Thai business organisations. This chapter reports on the scope of this research, and the significance of and background to issues related to ICT risk management in these organisations. The rationale, objectives and research questions are introduced. Finally, this chapter outlines the thesis structure.

1.1 Background

This research highlights success factors based on the COBIT framework and the ISO/IEC 17799 standard in organisations for planning ICT risk management. Siponen and Willison (2009) argue that there is little research that proposes how the two standards can fit together in the context of an integrated approach to ICT risk management.

Successful ICT risk management in organisations has been a concern for businesses over the past 10 years. For example, a computer security institute research shows that $202 million were lost in computer crime in 2003 (McAdams 2004). A report by the Audit Commission of the United Kingdom identifies increases in ICT abuses and frauds, regardless of whether organisations have concrete ICT governance arrangements in place (Audit Commission 2005). A government report in the USA shows that over 80 percent of ICT development projects have failed in whole or in part due to poor ICT risk management (Center for Technology in Government 2008). ICT risks have been identified for business. They are operational and associated technical and strategic risks.

Firstly, operational risks can be resulted from the skills and abilities that human resources contribute have been shown to help organisations boost business performance in dealing with risk (Willcocks et al 2006). Human resources are imperative factor in organisations because their roles and responsibilities directly affect the processes of information flow and audit related to risk management (Willcocks et al 2006). Secondly, ICT risk management is defined in terms of its ICT and information security components to deal with technical or security risks (Smith & Eloff 2002). ICT component refers to the

scope of the ICT domain where ICT produces data through input, processing, output (IPO) processes and disseminates information to internal and external parties. In contrast, information security component is focused to ensure that data and information are protected through „identification and authentication, authorization, confidentiality, integrity and non-repudiation“ (Smith & Eloff 2002, p. 268). From both components, technical or security risks can be resulted from any ICT infrastructure and security systems breaches. Therefore, management of ICT process and information security process is the focus in organisations to pay more attention on. Lastly, strategic risk can be derived from information system architecture (ISA) development that is difficult for users at the conceptual level (i.e. strategic plan), at the logical level (i.e. process and method of work) and/or at the physical structure level (i.e. the action plan or the operational plan) (Segars and Grover 1996). This implies that the setting of the strategic plan at the corporate level and the setting of the action plan at the operational level may not be clearly defined and communicated to users due to the inclusion of difficult or complex strategic terminology, and documentation may therefore be misinterpreted or difficult to interpret (Segars and Grover 1996). Therefore, the strategic plan and the operational plan are emphasised on dealing with ICT risk management.

1.2 Research motivation

To effectively minimise and control ICT risks, ICT risk management policies and strategies need to be developed and implemented in organisations. ICT risk management refers to the process aimed at aiding enterprises to achieve new business changes, future investment in information and information systems and ‘an increasing dependence on information and the systems that deliver this information’ (Lainhart 2000, p. 5; Lainhart 2001b; Jordan & Silcock 2005).

Much research has been done to examine the issues around ICT risk management in organisations (Segars & Grover 1996; Teneyuca 2001; Coles & Moulton 2003; Solms 2005b). Traditional ICT risk management is more concerned with protecting the information assets of an organisation based on the eight categories of ICT risk classified by the International Federation of Accountants (IFAC 1995) and the Institute of Internal Auditors’ Professional Standards (IIA 1993). Lainhart (2001b) argues that ICT risk management should be a senior management concern, and that they must provide the processes, policies, procedures and strategies to deal with ICT risks. Such an approach facilitates a top-down methodology for identifying, evaluating, minimising and controlling potential ICT risks in organisations (Lientz & Larssen 2004), which focuses on control of an entire organisation through implementation of the ICT risk management process.

The Control Objectives for Information and related Technology (COBIT) framework is representative of this kind of risk management approach to addressing ICT risk management. The COBIT framework takes a holistic view of the organisation (Lainhart 2001a) and focuses on a top-down strategy which is used to describe the business functions, processes and tasks to support senior management developing, implementing and maintaining ICT governance across the organisation (Robinson 2005; Solms 2005a). Adopting a top-down strategy to manage ICT risks in an organisation means that the organisation is concerned more with whole-of-business view than with technical solutions to ICT risk management. As a result the emphasis is on organisational structure and content (Solms 2005b). Existing research, however, shows that organisations appear to lack the required technical sophistication in their internal audit management when using this top-down approach (Viator & Curtis 1998; Hermanson et al. 2000). Clearly, delineate technical orientation and business orientation are part of the planning for effective ICT risk management.

In order to address this issue, a bottom-up approach to ICT risk management has also been developed and its impact reported in the literature (Solms 2005a). One representative of this bottom-up approach is the ISO/IEC 17799 (renumbered ISO/IEC 27002 in July 2007) standard for effective ICT risk management (Martinez et al 2010). The ISO/IEC 17799 standard is an information security governance framework which focuses on a detailed technical or bottom-up approach (Saint-Germain 2005; Solms 2005a). A bottom-up approach emphasises technical security and elaborates on all processes dealing with ICT risk in detail. It also provides an organisation with general guidelines on how the ISO/IEC 17799 standard can be utilised to control, prevent and mitigate ICT risks.

This research investigates the current profile of ICT risk management used in Thai organisations to understand the social reality of this phenomenon, and to identify the success factors emerging from the adoption of either or both the COBIT framework and the ISO/IEC 17799 standard for ICT risk management. The research will use the outcomes of that evaluation to develop a successful ICT risk management (SICTRM) model based on both the COBIT framework and the ISO/IEC 17799 standard.

This research is particularly important for Thai businesses because the trend in the adoption of, and thus demand for, ICT in Thailand has increased every year since 1998 (Satanasathaporn 2007), yet no research has been undertaken to evaluate its impact in relation to risk. Thai businesses have expanded their business transactions online and thus now communicate through cyberspace (Satanasathaporn 2007). As a result, the disadvantages of ICT adoption in Thailand have been exposed, and the weaknesses of ICT now need to be reduced due to an already recognised weakness in corporate governance in the country (Johnson et al 2000). The weakness in corporate governance

in Thailand reported during and since the East Asian Financial Crisis of 1997 (Mitton 2002) affects all areas of organisational operation. Therefore, it is imperative that there is an investigation into the way Thai businesses handle risk. Moreover, Thai businesses have not encountered an ICT adoption crisis which would highlight the impact of any lack of advance ICT planning for dealing with ICT risks (Thuvasethakul & Koanantakool 2002).

In relation to ICT, the National Electronics and Computer Technology Centre (NECTEC 2003) of Thailand announced that four laws relating to data protection, national information infrastructure, computer crime and electronic funds transfer have been in place since 2001 to force Thai businesses to comply with improved standards of operations using ICT and to reduce the risks associated with ICT adoption. In complying with these laws, it is believed that 'these laws should lay down sufficient legal framework for Thailand to enter the new economy with more confidence' (Koanantakool 2000, p. 9). However, all of these laws have not been sufficiently enforced to compel Thai organisations to report the impacts of ICT activities to the appropriate regulators. These regulators include the Stock Exchange of Thailand (SET) and the Securities and Exchange Commission (SEC) of Thailand. Up until 2009 the only effective reporting related to corporate governance (SET 2009). It is therefore vital that the National ICT Policy in Thailand also consider the issue of corporate governance (NECTEC 2003).

Corporate governance has been shown to be of significant concern when an organisation is dealing with ICT risk management (Farrar 2005). Regulated corporate governance was only introduced to the banking industry in Thailand following the Asian Financial Crisis of 1997. This regulation was adopted by the central bank, the Bank of Thailand (Vongvipanond 2004). Since then these same regulations have been adopted by all Thai organisations registered with the SET. In the corporate governance regulatory setting in Thailand, risk management has also been introduced as a means of helping an organisation respond to strategic risk through, for example, a 'long-term strategic plan and short-term business plan', and respond to credit risks, for example, 'Basic prudential rules as laid out in the *Commercial Banking Act* such as large exposure of loan and investment, concentration of loan to single group or borrowers, prohibition of connected lending to directors or bank executive and families persons or legal entity in which bank have equity share, continued to be strengthened after crisis' (Vongvipanond 2004, p. 6). Therefore, risk management has become critical for all Thai businesses. Yet there has been less concern with ICT risk and little evaluation of its effectiveness.

ICT risk management has more recently, however, become a focus in risk management in Thailand because the Royal Thai Government was concerned about trends in computer crime. As a result the Royal Thai Government passed a new law on computer-related offences, as the *Computer Crimes Act 2008* (AHRC 2007). In addition, banks in Thailand moved quickly in the area of risk management, especially ICT risk, as this was a prime

area of concern in terms of crime initiated using ICT (ZDNetAsia 2007). Symantec saw this is an opportunity to introduce the Symantec ICT Risk Management Report to the Thai banks as an outsourced security and security incident management system (ZDNetAsia 2007). The Symantec ICT Risk Management Report includes recommendations on the effectiveness of both the COBIT framework and the ISO/IEC 17799 standard in dealing with ICT risks. The Director of Symantec in Thailand further added that its products were first introduced to the Thai banking and telecommunication sectors, before expanding to other business sectors in Thailand (ZDNetAsia 2007).

This research is important for Thai businesses as it provides them with information and data to consider for the development of their own blueprints for handling ICT risk management. This research was undertaken to gain detailed knowledge of practices in ICT risk management in Thailand, particularly in regards to the use of either, or both, the COBIT framework and the ISO/IEC 17799 standard for successful ICT risk management.

1.3 Research objectives

This research is aimed at investigating how structured approaches to ICT risk management are used successfully in practice in Thai businesses. The research will explore and explain how business and technical strategies are planned and conducted in Thai business organisations to achieve successful ICT risk management. More specifically, the research is focused on the development of a single management framework for dealing with ICT risk management in Thai business organisations. Moreover, in this regard the COBIT framework itself stipulates that its framework can complement other standards and frameworks (ITGI 2007), although there is no research that proposes how they can fit together in the context of a structured approach to ICT risk management (Tshinu et al. 2008; Siponen & Willison 2009).

Therefore, the research objectives are:

- To investigate the current profile of ICT risk management in organisational practices in a sample of Thai businesses,

- To identify and then model the success elements of ICT risk management in Thai businesses.

1.4 Research questions

To achieve the objectives of the research, a number of research questions are developed.

The main research question is:

- What factors determine successful ICT risk management in a business organisation in the Thai business context?

Three subsidiary questions are developed to support this major question, as follows:

- What are the current profiles of ICT risk management in Thai businesses?
- How are ICT risk management concepts applied in those Thai businesses? and,
- What success factors can be identified for successful ICT risk management derived from the adoption of the COBIT framework and the ISO/IEC 17799 standard?

The main research question is developed to assist the researcher to explore an understanding of ICT risk management. The three subsidiary questions are included to assist the researcher to explore in greater depth the phenomenon of ICT risk management. All of these questions are considered imperative to gathering the knowledge required to develop a model of successful ICT risk management for business organisations.

1.5 Thesis structure

Chapter 2 Literature review

This chapter provides a review of the literature related to ICT risk management in organisations from both the academic and practitioner perspectives. The chapter begins by discussing ICT risk management implemented and developed by organisations, including risk management processes, risk management control and risk management planning to dealing with ICT risks, including nonstandardised practices. Furthermore, standardised practices are discussed, based upon ICT governance (i.e. the COBIT framework) and information security (IS) governance (i.e. the ISO/IEC 17799 standard) which are used to deal with ICT risk management in organisations. The chapter concludes with a discussion of the dilemma created by structured approaches to ICT risk management which require further exploration.

Chapter 3 Research methodology

This chapter presents a discussion of the research methods, research design, and data collection and analysis techniques used in this research. The chapter begins with an explanation of the rationale behind the selection of research paradigm, research methodology and research design, including its basis in the literature. The chapter

concludes with a discussion of the data collection and analysis techniques used in both the qualitative and quantitative methods that were adopted in order to target the participants and sample appropriate to this research.

Chapter 4 Case studies in Thai business adoption of ICT risk standards: Cases A–C

This chapter reports on the interviews undertaken in the first part of this research. The chapter explores and presents understandings of the phenomenon and practice of ICT risk management in different types of Thai businesses as gathered from the interviews. The analysis of the qualitative data uses thematic and content analyses to capture the main processes regarding ICT risk management in the multiple case studies. Key factors are identified that relate to ICT risk management in practice.

Chapter 5 Case studies in Thai business adoption of ICT risk standards: Cases D–F

A discussion of the findings of further interviews undertaken in Thai businesses is presented in this chapter to explore understandings of ICT risk management practice. All case studies in this chapter are international consulting firms. The practices of ICT risk management in this chapter are then discussed based on both organisational (i.e. case studies' practices) and consulting perspectives (i.e. their clients' practices). The analysis of this chapter also uses thematic and content analyses to capture the main process regarding ICT risk management. Key factors are also identified that relate to ICT risk management in practice.

Chapter 6 Phase II: Survey development

This chapter begins with a comparative analysis of case studies A, B, C, D, E and F by comparing themes derived from Chapters 4 and 5. The key conclusions from Chapters 4 and 5 are revealed to facilitate the development of the model for dealing with ICT risk management in an organisational context. The last part of this chapter outlines the development of the survey instrument based on the findings from both the existing literature and from the analysis of the interviews reported in chapters 4, 5 and this chapter. The mapping of the constructs drawn from the interview findings with the COBIT framework and the ISO/IEC 17799 standard is discussed in order to generate a conceptual model, which are validated in Chapter 7.

Chapter 7 Survey of Thai business adoption of ICT risk standards

This chapter begins by describing the statistical analysis of the data screening, item parcelling, the response rate, demographic statistics and the reliability of the instrument. The chapter elaborates on the quantitative research undertaken via a mailed survey. The chapter explains and then confirms or disconfirms the constructs in the conceptual model of ICT risk management (presented in Chapter 6) used in Thai organisations by using

structural equation modelling (SEM). The report on the validation begins by describing the statistical validity tests used—content validity, construct validity, convergent validity, discriminant validity, measurement validity and nomological validity—to test the sense and meaning of the structural model. The chapter concludes with a discussion of the successful ICT risk management model (SICTRM) and the relationships among variables in the model.

Chapter 8 Discussion and Conclusion

This chapter revisits the research objectives and research questions in order to confirm whether they have respectively been achieved or answered in this research. Multiple case studies and the survey results are compared and summarised to propose the key success factors of ICT risk management as evidenced by Thai organisations. The chapter ends with a consideration of the limitations of the research, suggestions for future research and the conclusion.

Chapter 2
LITERATURE REVIEW

This chapter reviews the existing literature to frame the main theory that underpins this research. The chapter is divided into five parts. Firstly, ICT risk management as an unstructured approach is discussed through a holistic consideration of its components. Secondly, the risks related to ICT are described as the main focus of this research. Thirdly, the success factors within an unstructured approach to ICT risk management are explored as the primary source of ICT risk management. Fourthly, a structured approach to ICT risk management using ICT governance (the COBIT framework as 'the top-down approach') and IS governance (the ISO/IEC 17799 standard as 'the bottom-up approach') is discussed. These standards are widely used to guide organisations that are dealing with ICT risks. Lastly, the merits of using structured approaches to ICT risk management are discussed in terms of the success factors for developing an ICT risk management plan that drives effective and efficient organisational performance.

2.1 ICT risk management

Several research papers have shown that ICT risk management must be practised in the organised way in order to avoid and/or prevent risks (Dhillon & Backhouse 1996; Viator & Curtis 1998; Carnaghan 2006). Badenhorst and Eloff (1994, p. 411) suggest that the scope of a risk management process should be focused on 'risk identification, risk analysis, risk assessment (e.g. risk evaluation and risk allocation), risk resolution (e.g. risk decision, risk conclusion, risk financing, risk regulation and risk control) and risk monitoring (e.g. risk administration)' (p. 415). Cha et al. (2008) also agree that a risk management process must include risk identification, risk assessment, risk treatment, risk monitoring and risk reassessment. Whereas Bandyopadhyay et al. (1999) highlight that the four major elements of ICT risk management process are risk identification, risk analysis, risk reduction measures and risk monitoring. According to them, all need to be applied to 'the planning stage of system development and to continue throughout the development process' (Bandyopadhyay et al. 1999, p. 438).

Risk identification must occur at 'the application level, the organizational level and the inter-organizational level' (Bandyopadhyay et al. 1999, p. 438). Identifying risk at the application level accounts for the technical risk or implementation failure of ICT applications, including 'internal threats to ICT assets' such as 'unauthorized physical access and system abuse', and external threats such as 'natural disasters, acts of competitors, hackers and computer viruses'. Risk identification at the organisational level needs to account for 'the impact of ICT throughout all functional areas of the organization'. This level focuses on strategic risks which might obstruct an organisation seeking to sustain a competitive advantage 'from the deployment of ICT applications on a long-term basis' (Bandyopadhyay et al. 1999, p. 439). Lastly, identifying risk at the inter-organisational level is primarily focused on external telecommunications, including electronic data interchange (EDI) when an organisation places transactions online with suppliers, customers and distributors. How this identification of risk takes place relates to risk analysis processes that are integral to risk management. McEvoy and Whitcombe (2002, pp. 91-92) further add that risk identification is dependent on understanding the ICT environment in order to 'identify the information assets that the service must manage' and to 'understand the physical architecture of the system within which this information is stored and manipulated'. Moreover, it also helps assess information intensity in terms of the value chain (processes and systems) and products (information) and determine the staff roles and responsibilities in the organisational structure (McGaughey et al. 1994).

On the other hand, Gerber and Solms (2005) argue that risk identification is an integral part of risk analysis which enables an organisation to quantify or estimate both the probability of a risk occurring and the magnitude of its consequences. However, risk analysis has been defined either as a quantitative methodology based on 'expected value analysis related to ICT risks', or as a qualitative methodology based on 'descriptive variables for analysing ICT risks', or a combination of the two, based on 'estimated value of ICT assets as well as probability estimates for the realization of various threats' (Bandyopadhyay et al. 1999, p. 440). Gerber and Solms (2005) further add that the main purpose of risk analysis is to help an organisation identify sources of risk which derive from a combination of asset, threat and vulnerability.

Risk-reducing measures are defined as helping an organisation prevent the occurrence of losses as a result of either the internal environment (i.e. data security, computer viruses, strategic risks) or the external environment (i.e. natural disasters, computer viruses and legal risk) (Bandyopadhyay et al. 1999). Badenhorst and Eloff (1994) argue that such measures rely on risk assessment (e.g. risk evaluation and risk allocation). Risk-reducing measures focus on investigating how ICT might help an organisation deal with potential risk and developing a plan based on risk identification and risk analysis

(McGaughey et al. 1994). Once risks are identified and assessed, the right risk minimisation strategy needs to be applied (Bojanc & Jerman-Blažič 2008). Such strategies include avoiding, reducing, transferring and accepting (Stoneburner et al. 2002). These four strategies are seen as minimising the risks after an organisation has performed a risk management process. Avoiding entails the elimination of the sources of risk, that is, the threats and attacks (Bojanc & Jerman-Blažič 2008). The reducing strategy engages appropriate technology or tool implementation or appropriate security policy adoption to mitigate an asset's exposure to risk (Bojanc & Jerman-Blažič 2008). Transferring is a strategy whereby an organisation partially shifts its responsibilities to outsourcing security agents who take action on the identified risks (Bojanc & Jerman-Blažič 2008). With the accepting strategy, an organisation accepts the costs of risk retention embedded in the security measures, but still seeks to keep such risk under control (Bojanc & Jerman-Blažič 2008).

Risk monitoring is the last component which helps an organisation ensure that risks originating from potential countermeasures are controlled appropriately (Bandyopadhyay et al. 1999). It includes 'a continuing audit function' that relates to 'a number of audit tools such as Computer Assisted Audit Tools and Techniques (CAATT), and measurement tools for tracking website[s]' (Bandyopadhyay et al. 1999, p. 443). Monitoring of risk has often led to the development of control measures.

According to the literature discussed above, the ICT risk management process has been written in risk management standard which covers context establishment, risk identification, risk analysis, risk integration, risk evaluation, risk treatment and risk monitoring in the literature for the past decade (Baccarini et al. 2004; Moeller 2007). The investigation of the ICT risk management process is one component of ICT risk management. Other components (e.g. risk management control and risk management planning) of ICT risk management are delineated next.

Badenhorst and Eloff (1994, p. 412) suggest that the scope of ICT risk control is focused on 'ICT, information security (IS) and risk management' as defined in the Target Optimum Portfolio Management (TOPM) model. The scope of ICT can be categorised into object and subject groups. The object group refers to information, meta-information (e.g. a database), and the technology and facilities domains which are ICT resources (Badenhorst & Eloff 1994). Moreover, ICT risk control of technological processes is dependent upon internal systems which relate to both business and ICT processes (McGaughey et al. 1994; Coles & Moulton 2003). By aligning business process with ICT process, Calderon and Dishovska (2005, p. 21) argue, what is termed Business Continuity Management (BCM) can be used to allow an organisation to address 'a wide variety of risks and views ICT as a business process enabler'. In so doing, an organisation must document and demonstrate BCM processes across its business

operations in order to ensure that all business and ICT functions can continue with minimal disruption after an incident (Calderon & Dishovska 2005). Cha et al. (2008) assert that BCM processes are defined as initiation; requirements and strategy; implementation; and operations management. Initiation entails an organisation developing and setting its business continuity policy (its staff roles and responsibilities, the schedule of the policy, and other principles and guidelines) to provide the basis for BCM activities (Cha et al. 2008). The requirements and strategy process involves undertaking a business impact analysis which helps to identify the interruption of business processes and to assess the potential loss caused by an incident so that BCM strategies can be developed based upon the results of such assessment (Cha et al. 2008). Implementation is dependent upon the BCM strategies an organisation adopts to 'develop and implement contingency plans (the incident response plan, the disaster recovery plan and the business continuity plan) to ensure the continuance of its critical business at an acceptable level' (Cha et al. 2008, p. 111). Lastly, operations management is aimed at ensuring that an organisation can maintain BCM processes as part of business as usual. By maintaining BCM processes, 'appropriate awareness, education or training programs' are provided in order to update 'BCM policies and plans', keeping up with 'organization[al] changes and system enhancements' (Cha et al. 2008, p. 111).

The subject group refers to decision-making related to human resources in an organisation such as organising, staffing, directing and controlling, in combination with the business functions and transaction domains (Badenhorst & Eloff 1994). Coles and Moulton (2003) argue that few companies properly implement ICT risk control in ICT risk management. This weakness derives from deficiencies in the processes and/or approaches as well as the tools used. These deficiencies include a lack of technical sophistication in internal audit management, a lack of attention to ICT management, a lack in the technical abilities of individual internal auditors and a lack of resources (Hermanson et al. 2000). Likewise, for many organisations, there are only internal auditors who are responsible for ICT control rather than specialised or skilled auditors (Hermanson et al. 2000). This implies that business process managers do not participate in the ICT aspects of risk management from the technical angle in the business planning of the organisation. Coles and Moulton (2003) therefore recommend that an organisation needs to follow the business process in combination with information risk management based on a value chain as two elements of Business Process Information Risk Management (BPIRM). A value chain in the BPIRM model is considered to be based upon initiating, defining, assessing, implementing, managing and confirming processes to ensure that: quality control, corporate policy, external laws and regulations are addressed (governance); the governance function is properly executed by business leadership (reassurance); ICT policies, guidance and compliance meet corporate

governance requirements (ICT process leadership); those people who direct ICT processes and application are properly allocated their roles and responsibilities (ICT people resources); transforming the process of data (input) to information (output) is controlled properly through data/sub-processes/applications/information, infrastructure and technology; and third parties (e.g. an external ICT auditor) and the suppliers of ICT are available when required (Coles & Moulton 2003).

Lastly, the scope of IS security is the focus to prevent, recover and mitigate the threat, vulnerability and potential loss impacts of risks occurring in relation to human resources security, physical access security, or theft of an organisation's information and information resources (Badenhorst & Eloff 1994). Thus, this model focuses on ICT and IS by carrying out risk management processes as a 'technological framework for an ICT risk management model' (Badenhorst & Eloff 1994, p. 412). Another example of risk management control in IS security is known as Structured Risk Analysis (SRA). McEvoy and Whitcombe (2002, p. 88) suggest that SRA is 'a method to help an organization take rational steps to improve their information security'. Furthermore, SRA also enables an organisation to deliver confidentiality, integrity and accountability (CIA) to information security. To achieve a successful SRA, an organisation needs to address: the business context (e.g. the decision-maker must justify their decisions in relation to information security resources); technical grounding (e.g. systems analysis and design must ensure that information services and the physical system are delivered intact to the appropriate users); separation of concerns (business and technical concerns need to be separated according to the relevant threats pertaining to them); support for quantitative analysis (the budget for information security should be quantified and allocated); turnable analysis (controlling the levels of the analysis, appropriate to particular corporate circumstances); evolution (evolving the methods of the change used to attack problems and perform countermeasures); maintainability (ensuring the risk analysis model is adequately flexible to allow for changes to operations and services); and openness (being open to changing standards in relation to software purchasing and licensing) (McEvoy & Whitcombe 2002).

ICT risk management planning refers to the management of policies, technical means and active monitoring which all function to maintain control and reduce vulnerabilities or threats as risks related to ICT (McEvoy & Whitcombe 2002). McEvoy and Whitcombe (2002) further articulate that: policies 'must be developed, [and] applied to define who can have what kind of access to which information and infrastructure components'; procedures 'must define the controls around such access'; technical means 'must be deployed to enforce policies and procedures'; and active monitoring must 'detect serious or systematic attempts to circumvent the policies and procedures' (McEvoy & Whitcombe 2002, p. 89). This idea is based on the adoption of the structured risk analysis (SRA)

model to successfully manage information security risk. Nevertheless, the SRA model itself mainly focuses on information security; it is not able to provide a broad conceptualisation regarding ICT risk management planning.

Drawn from the discussion above, a summary of the components of ICT risk management is presented in Table 2-1. As revealed in Table 2-1, risk management process, risk management control and risk management planning are three major areas within ICT risk management under study in this research. However, risk management planning remains ill defined. The next section discusses the sources of risk related to ICT in order to help the researcher conceptualise the entire pipeline of ICT risk management planning in an organisation.

Table 2-1: Summary of the components of ICT risk management

ICT risk management							
Study	Badenhorst and Eloff (1994)	McGaughey et al. (1994)	Bandyopadhyay et al. (1999)	McEvoy and Whitcombe (2002)	Coles and Moulton (2003)	Gerber and Solms (2005)	Cha et al. (2008)
Model	Target Optimum Portfolio Management (TOPM)	Value Chain		Structured Risk Analysis (SRA)	Business Process Information Risk Management (BPIRM)		Business Continuity Management (BCM)
Concern	- Technicality - Functionality			- Information security	- Business perspective - Information technology		- Business functions - ICT functions
Risk Management Control	- Information communication and technology ▪ ICT resources management - Information Security ▪ Human resource management	- External factors (threats) - Internal technological processes (vulnerabilities of assets)		- Information security resources ▪ Confidentiality ▪ Integrity ▪ Accountability	- Business process - Information communication and technology process		- Asset management - Relationship management - Incident management
Risk Management Process	- Risk identification - Risk analysis - Risk assessment - Risk solution - Risk monitoring	- Risk planning ▪ Strategic ICT planning - Risk control ▪ Risk identification ▪ Risk analysis ▪ Risk assessment	- Risk identification - Risk analysis - Risk reduction measures - Risk monitoring	- Risk identification - Risk assessment	- Initiating business process - Define business process, information and IT requirements - Assessing risk, creating risk profile for process and applications - Implementing control solutions - Managing operational control - Confirming and redefining adequacy of controls	- Risk analysis ▪ Risk identification ▪ Risk estimation ▪ Risk evaluation - Risk management ▪ Controlling and monitoring risk analysis	- Risk identification - Risk assessment - Risk treatment - Risk monitoring - Risk reassessment
Risk Management Planning				- Policy - Procedures - Technical - Active monitoring		- Planning - Monitoring - Controlling	- Business continuity policy

2.2 Risk related to ICT

ICT-related risks result from uncertainty around several aspects of ICT operations, from the probability of business losses or failure, and from negative outcomes originating from both internal and external environments (Straub & Welke 1998; Teneyuca 2001; Levine 2004; McAdams 2004; Shedden et al. 2006).

In general, three major ICT-related risks have been identified for business: operational risks, technical risks, and strategic risks (Segars & Grover 1996; ITGI 2005; Shenkir & Walker 2006). Operational and associated technical risks result from improperly performing ICT operations such as: (a) loss of computer assets; (b) inaccurate record keeping; (c) increased risk of fraud; (d) loss or theft of data; (e) privacy violations; and (f) business disruption (Willcocks & Griffiths 1994; Straub & Welke 1998; Warren et al. 1996; Gelinas et al. 2005; Hawkins et al. 2003; Ward 2005; Ciborra 2006; Hughes 2006b; Pinder 2006; Ravenel 2006; Shenkir & Walker 2006). This risk implies that 'internal processes, people and system[s]' are controlled inadequately (Basel 2005, p. 140).

Hawkins et al. (2003) use the report of the US Department of Homeland Security to demonstrate that preventative actions are needed to protect information assets. Moreover, securing information assets must be a top priority in cases where the business transactions are carried out online (Hawkins et al. 2003). Hawkins et al. (2003, p. 23) found that '44.33 percent of the respondents' in a Computer Security Institute (CSI) security survey attested to '$455 million in financial losses due to computer breaches'. Thus, security breaches have become a major threat requiring that organisations develop operational security to deal with operational risk related to information security (Hawkins et al. 2003). This implies that operational risk affects technical risk and vice versa, and that both risks can be managed simultaneously.

Operational risks are derived from both external and internal processes (Willcocks & Griffiths 1994). With regard to internal processes, ICT risks are 'a result of distinctive human and organisational practice and patterns of belief and action. This is because certain features are inherently more risky than others' (Willcocks & Griffiths 1994, p. 225). Moreover, the skills and abilities that human resources contribute have been shown to help an organisation boost business performance in dealing with risk (Willcocks et al. 2006). Straub and Welke (1998) assert that operational risk (e.g. systems risk) occurs when an organisation does not adequately protect its information and information systems against certain kinds of damage or loss. The reason for such inadequate protection or preventative planning perhaps lies in the fact that 'information security continues to be ignored by top management, middle management and employees alike' (Straub & Welke 1998, p. 442). Ward (2005) also argues that people are an important

factor in an organisation because their roles and responsibilities directly affect the processes of information flow and audit related to risk management. Specifically in relation to ICT, the role of ICT staff is especially significant regarding technical matters (e.g. information security) and in determining ways to prevent computer abuses by staff or by improperly performed ICT operations (Ward 2005).

Bojanc and Jerman-Blažič (2008, p. 216) state that 'security risks are present in the organization's information system due to technical failure, system vulnerabilities, human failures, fraud or external events'. This implies that information security systems are invested in and designed to protect the confidentiality, integrity and availability of information assets.

Strategic risk originates from the planning and implementation of ineffective ICT strategies, including or as a result of:

(a) the potential likelihood of failure through a lack of strategy;
(b) the risk consequence of a lack of strategy;
(c) the lack of specific management of ICT risks;
(d) the nature of management perceptions;
(e) management processes inside the company;
(f) the responsibility of ICT audit and control; and
(g) the complexity of systems (Segars & Grover 1996; Baccarini et al. 2004).

Baccarini et al. (2004) also suggest that project management, as the management strategy of risk reduction, can help organisations deal with strategic risks in IT projects. However, risk management strategy is then, they argue, project management that focuses more on project management processes than technical processes (e.g. technical risk) (Baccarini et al. 2004).

Segars and Grover (1996) note that strategic risk can be derived from information system architecture (ISA) development that is difficult for users at the conceptual level (i.e. strategic plan), at the logical level (i.e. process and method of work) and/or at the physical structure level (i.e. the implementation plan). At the conceptual level the strategic direction of an organisation may not be clearly communicated to staff due to the inclusion of difficult or complex strategic terminology, and documentation may therefore be misinterpreted or difficult to interpret. This involves a 'lack of [a] concrete or understandable strategic plan, no ongoing assessment of strategy, [a] lack of interest by top management in IS planning and [a] lack of skills or methodologies for constructing enterprise models' (Segars & Grover 1996, p. 387). In other cases, an organisation simply has no strategic plan or an unstructured or incomplete strategic plan. In the latter case, Segars and Grover (1996, p. 389) add that the information system planners seem overwhelmed by the scope and complexity of information created and used throughout

the enterprise, for example, 'scope of requirements [is not] identified for data and processes, planning [is not] focused on supporting the status quo versus redesigning processes and methods of work, and [there is a] lack of skill or methodologies for constructing logical models' at the logical level. The scope and complexity of information created and used throughout the enterprise lead to 'information system planner does not feel confident in their approach to logical design and therefore information system planner is not certain that architectural models contained the right information to guide development efforts' (Segars and Grover 1996, p. 390). Lastly, operations are affected by the strategic plan, processes and methods of work which relate to the 'semantic gap[s] between logical and implementation plans'. Therefore, the strategic plan influences the logical thinking behind designing processes and methods of work. This then impacts on the implementation plans at the operations level in cases where there is no strategic plan or only an unstructured or incomplete strategic plan. According to the discussion above, it can be seen that ICT risks can emerge from operational risk, technical risk and strategic risk as shown in Table 2-2.

Table 2-2: Summary of key factors based upon the sources of risk

Type of risk	Source of risk	Key Factor
Operational and associated technical risk	- Loss of computer assets - Inaccurate record keeping - Increased risk of fraud - Loss or theft of data - Business disruption - Privacy violations - Computer breaches - Inadequate protection of information and information system - Unclear roles and responsibilities - Technical and human failures - System vulnerability - Fraud or external events	- Asset management - Human resource management - Information security management - Information technology management
Strategic risk	- A lack of strategy - A lack of specific management of ICT risks - The nature of management perspectives - Management processes failure - The responsibility of ICT audit and control - The complexity of systems - Unclear strategic plan - Unclear operational plan - ICT project management failures	- Organisational strategy - Organisational policy - Planning regarding strategic and operational plans

The sources of ICT risk reflect the key factors which are discussed in the next section.

2.3 Key factors in ICT risk management

The best approach to ICT risk management in an organisation is to approach problems from various perspectives including consideration of both the internal and external environments (McGaughey et al. 1994). ICT risk management needs to be examined in the context of all organisational processes, including organisational structure; process

and control; and technical implementation of risk management strategies and policies (Benaroch et al. 2006). The following paragraphs discuss the key factors which are the bases for of ICT risk. These insights will assist organisations to improve organisational planning for dealing with ICT risk management.

2.3.1 Human resource management

Risk consequences based on risk management actions are embedded in institutional and organisational structure (Ciborra 2006). Organisational structure engages with risk management through human resource management and its associated security issues. Ciborra (2006, p. 1348) argues that the risk management process (e.g. risk assessment) poses a dilemma because the assessor (e.g. decision-maker) must face 'the ramifications of a lack of knowledge, the role of biased data when assessing risk in organizations and the influence of internal politics'. Moreover, decision-makers are required to set the policy to deal with different and/or multiple categories of identified risks (Hughes 2006a). This implies that risk management planning, as in planning organisational structure to incorporate risk management, must be undertaken. Organisational structural planning for risk management provides a roadmap of the ICT required to support and enhance the business direction of an organisation. It also identifies the human resources required to implement the plan (Figg 1999).

Hughes (2006a) adds that an organisation must build the internal competence to manage ICT risks on its own. An organisation needs to develop the knowledge and processes required to manage its own ICT risks because most organisations have a poor awareness of their ICT exposure to risk. To develop the processes required to raise awareness of these issues, senior managers need to 'develop an awareness of the nature of the different ICT risks to the business; quantify the impact to their business resulting from the loss of information or access to application; understand the range of tools available to manage ICT risks; align the costs of ICT risk management to the business values; and build systematic and corporate capability to manage security risk' (Hughes 2006a, p. 36). Levine (2004) also supports the view that ICT risk management must take into account people, process and systems, including organisational factors such as corporate culture and employees. Organisational factors are considered to include the roles and responsibilities of staff; risk awareness; and the access control for authorised employees in an organisation. Raising awareness among staff should focus on human resources, in particular regarding information security (e.g. unauthorised people), availability (e.g. human error, configuration changes, lack of redundancy in architecture), recoverability (e.g. disaster recovery plan embedded in business continuity plan), performance (e.g. distributed ICT architectures), scalability (e.g. balancing costs and benefits of ICT

investment), and compliance (e.g. regulatory requirements from both inside and outside an organisation) (Hughes 2006a).

Straub and Welke (1998) argue that system risk is mainly in the area of information security matters, and that managerial guidelines on ICT risk in general are focused on human resource management and risk management processes. Human resource management is considered significant because an organisation needs senior management support in seeking to gain a thorough understanding of organisational vulnerability and of the resources required to secure organisational systems (Straub & Welke 1998). It is necessary that senior management understand the security actions and can thus integrate security planning into information security policy as organisational standards, and that users are trained and educated regarding security awareness so that organisational standards can be reviewed and updated as needed (Straub & Welke 1998). Hughes (2006a) further claims that managing ICT risks must focus on a combination of process, people, technology and information. The ICT operational process helps an organisation design, execute and measure systematic approaches, standards and frameworks to determine the best practice for ICT operational processes—such as those based on the standards of the International Organization for Standardization (ISO)—in order to mitigate ICT risks (Hughes 2006a). Staff at all levels can also help reduce risks. Therefore, training programs; clarification of roles and responsibilities; and the identification of specific authority for specific roles should be provided for all staff (Hughes 2006a).

Longstaff et al. (2000, p. 44) define ICT risk management as associated with protecting information and information systems in both the 'structural-based' and 'human-based' dimensions. In particular, the human-based domain includes protecting institutions, organisations, culture and language which explicitly relate to operational functions (Longstaff et al. 2000). By protecting human-based domains, the operational element is required for dealing with risk assessment and risk management. On the other hand, the structural-based domain involves protecting hardware, structures and facilities (which explicitly relate to ICT management and IS management) (Longstaff et al. 2000). This is discussed in the next section.

2.3.2 ICT management and IS management

Smith and Eloff (2002, p. 268) argue that 'ICT risk management is defined in terms of its Information Communication and Technology (ICT) and Information Security (IS) components'. The first component, information communication and technology (ICT), refers to the scope of the ICT domain where ICT produces data through input, processing and output (IPO) processes and disseminates information to internal and external parties

(Smith & Eloff 2002). This component controls the capacity of ICT used in IPO processes, specifically in relation to ICT risks (Smith & Eloff 2002). Therefore, ICT used in IPO processes is limited to controlling the input of data, processing data to information and storing information in a database, as well as disseminating information to stakeholders and stockholders (Smith & Eloff 2002). Moreover, ICT related to ICT architecture helps an organisation define 'the strategy that drives, shapes and controls its architecture' when dealing with ICT risk management (Byrd et al. 1995, p. 39). Such strategy must allow computing, telecommunications, data and applications (ICT resources) to work together constructively (Byrd et al. 1995). ICT architecture is specified by what types of hardware and software are employed; where personnel, equipment, data and facilities are located; the levels of applications, data and procedural compatibility that exist across locations (e.g. department to department, business unit to business unit); and how locations are connected, coordinated, and controlled (e.g. telecommunications networking) (Byrd et al. 1995).

Both the physical security systems and the information communication and technology environment must be considered at both the higher employee levels (e.g. senior management) and the lower level (e.g. operations) to ensure the control of risk is effective (Schultz 2007). Schultz (2007) also provides guidance on how to mitigate ICT risks regarding physical security systems (e.g. devices, process control systems and ICT infrastructure). Firstly, he asserts that it is necessary to gather knowledge to understand the configuration of networks, systems and ICT infrastructure in order to respond appropriately to the problem (Schultz 2007). Secondly, conducting risk analysis is required to identify any vulnerability of assets that may be exploited for incorrect purposes, which might then lead to threats (Schultz 2007). Therefore, vulnerabilities, threats and the likelihood of each occurring must be identified. Moreover, risk assessment should also be conducted using penetration tests in order to target physical security systems around organisational networking. Thirdly, the problem must be reported to the management and audit functions. Senior management needs to understand and support the provision of resources necessary to protect against such problems. The internal auditor also needs to be informed to cover the particularities of the problem within the auditing area (Schultz 2007). Fourthly, senior management needs to develop organisational information security policies (e.g. an annual plan) to define the requirements regarding security issues for managers, technical staff and users. Fifthly, an action plan (e.g. outlining technical means) needs to be developed, implemented and tested to measure the level of appropriate security in an organisation. Sixthly, an organisation needs to integrate physical (e.g. ICT devices) and logical security (e.g. information security functions) because many of the risks to the logical system are also physical and vice versa. In terms of integration, an organisation needs to develop the relationships that allow physical security and information security functions to work

together. However, 'many senior managers are unaware that ICT security in their organizations is inadequate [or] what the consequences of vulnerability may be' (Byrd & et al. 1995, p. 41).

Thus, the second component, information security, must be focused on, ensuring that data and information are protected through 'identification and authentication, authorization, confidentiality, integrity and non-repudiation' (Smith & Eloff 2002, p. 268). This helps protect organisations' information relating to business processes and business transactions. By engaging with business processes and business transactions, an organisation can therefore secure data and information in both the ICT used and security services in order to manage ICT risks. Generally, risk management analysis involves the implementation of information security controls whereby a security officer targets users in order to perform a risk assessment (Straub et al. 2008). In doing so, unacceptable risk can be identified in order to determine possible countermeasures and options for dealing with such risk (Straub et al. 2008). Thus, decisions are made to determine a countermeasures procedure and appropriate security measures by teams of security experts and targeted users.

In the implementation of information security control in ICT risk management, knowledge of system requirements is essential to prevent threats and reduce risks created by the vulnerability of assets via human interference (Księżopolski & Kotulski 2007). Moreover, information security control helps an organisation protect information assets at every staff level from both internal and external threats (Anderson & Choobineh 2008). Through this process an organisation estimates the probability and impact of the potential risk based on 'the result of an information security incident caused by a threat affecting assets' (Księżopolski & Kotulski 2007, p. 254). System requirements include safeguard measures such as practices, procedures or mechanisms that prevent threats; reduce potential risk originating from the abuse of asset vulnerability; and mitigate the probability and impact of the potential risk (Księżopolski & Kotulski 2007).

By doing so, the operationalisation of information security control is focused on providing enterprise information security. Enterprise information security is classified into three main areas. Firstly, at the asset level, an organisation focuses on 'the incident(s), its characterization, and the threat-vulnerability combinations that can lead to potential losses' (Anderson & Choobineh 2008, p. 23). This implies that an organisation operationalises security tools and methods to detect and prevent potential damage at the technical level. For example, data management as an information asset is considered because in the process of the collection and archiving of historical data there is both expected loss and actual loss, and these processes must be maintained in order to prevent the same incident reoccurring in future (Levine 2004). Therefore, data quality derived from data management is a major challenge for an organisation because risk

managers need to make decisions in a timely manner based on accurate data. Therefore, an organisation needs to learn from the past in order to adapt its risk management processes in order to maintain the quality and accuracy of its data (Levine 2004).

At the operational level an organisation must codify best practices, 'technical solution[s], operational solution[s], information security awareness, threats identification and security requirement specification' in order to reduce ICT risks (Anderson & Choobineh 2008, p. 23). The aim of risk management is to achieve access control mechanisms and proactive threat assessment techniques as technical or operational solutions (Hayat et al. 2007). To preserve the confidentiality, integrity and availability of information, for example, it is recommended that context-based access control and compromised threat analysis be included in the information security risk management technology (Hayat et al. 2007). Context-based access control is used to protect a network from external environmental influences to prevent the threats posed by unauthorised external access (Hayat et al. 2007). This proactive method implies that information security management (e.g. access control) has to be considered by an organisation when undertaking ICT risk management. Furthermore, Milenkovic (2008) argues that access control is part of information security in relation to governance, risk management and compliance (GRC). In achieving GRC, roles and responsibilities (e.g. information security awareness) must be assigned certain levels of access in order to clearly define the main drivers in operational functions within an organisation (Milenkovic 2008). Milenkovic (2008) argues that role-based access control must be defined for all business participants (e.g. users, administrators, ICT persons and internal auditors) to comprehensively monitor the business processes around access control.

Lastly, at the strategic level an organisation has to provide 'an enterprise-wide perspective' which combines horizontal and vertical management approaches to protect against 'threats, vulnerability, [and] organizational impacts' across the organisation (Anderson & Choobineh 2008, p. 23). The following section discusses successful ICT risk management control.

2.3.3 Successful ICT risk management control

Finne (2000) asserts that ICT risk management is about ICT control which is embedded in business process. ICT control and business control are adopted to ensure that the design of policies, procedures, practices and organisational structures meets the business objectives and functions to prevent, detect and correct ICT risks effectively (Finne 2000). This implies that dealing with ICT risk successfully is dependent upon the control and management of overall risks in an organisation. Flowerday and Solms (2005, p. 604) argue that ICT risk management must include a system of internal control related to ICT

which is 'paramount to ensure the information's integrity'. A system of internal control particularly in ICT helps an organisation 'limit uncertainty and mitigate the risks to an acceptable level' (Flowerday & Solms 2005, p. 604). Managing information risks is part of organisational internal control that safeguards the accuracy of organisational internal information (Flowerday & Solms 2005).

Holzmann and Jorgensen (2001) assert that risk management control consists of prevention, mitigation and coping strategies in social risk management. Such strategies have previously been highlighted in relation to dealing with risks in terms of the social protection of labour markets, pensions and social assistance in a World Bank report. However, as Gallegos et al. point out they can also be adopted for use in ICT because risk management is a broad area which can be applied across disciplines (2004). In this regard, a prevention strategy is used to hedge the probability of adverse risk or negative occurrence by planning policy actions for risk prevention (Gallegos et al. 2004). A mitigation strategy is aimed at mitigating the impact of the risk by providing instruments for risk mitigation (Gallegos et al. 2004). A coping strategy is a means of minimising harm caused by a negative occurrence through the provision of a scheme of arrangements (Gallegos et al. 2004).

According to the National Institute of Standards and Technology (NIST), 'risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions' (Stoneburner et al. 2002, p. 4). This implies that risk management is a methodology that an organisation uses to balance its return on investment (ROI) of ICT (e.g. cost and benefit) and to protect its ICT systems and data from attack from threats in either the internal or external environments. Moreover, Stoneburner et al. (2002) assert that risk management entails processes around assessing risks, mitigating risks, and risk evaluation and assessment. It has also been implied that ICT risk management helps an organisation not only prevent but also mitigate and avoid risks occurring. Therefore, the objective of ICT risk management can be achieved through strategic application aimed at the mitigation, prevention and avoidance of risks (Bandyopadhyay et al. 1999). Success factors lead to the development of ICT risk management planning in an organisation. The following section discusses ICT risk management planning as a structured approach.

2.4 ICT risk management as a structured approach

In this research, a structured approach to ICT risk management refers to the use of a standard or framework for ICT risk management planning. The structured approach is based on a standard that lays out the business direction. The business direction is more

concerned with corporate governance and enterprise risk management when dealing with business risks. On the other hand, ICT does not concentrate on corporate governance to deal with ICT organisational risk. Berry et al. (2009, p. 11) argue that the rate of development of ICT has increased dramatically to support organisational processes over the past two decades, but 'the relationships between management control and new ICT remain underdeveloped both theoretically and practically' in terms of dealing with ICT risk. To effectively manage ICT risk in an organisation, corporate governance of ICT, ICT governance and IS governance are explored in the research to provide effective action planning for organisations (Sarens & Beelde 2006; Gotterbarn 2009). However, since the ISO/IEC 38500 is a new standard (published in 2008 while this research was being carried out), there has as yet been no research on the impact of its implementation (ISO/IEC 2008). Thus, this research focuses upon the available standards and frameworks by focusing on ICT governance and information security (IS) governance, which are discussed next.

2.4.1 ICT governance

ICT governance is a set of processes, procedures and policies that are the responsibility of senior management and the Board of Directors (ITGI 2007). Organisations use ICT governance to guide and control ICT in order to attain business goals and objectives while balancing ICT risks with return on ICT investment (Ridley et al. 2004; Smith & McKeen 2006). ICT governance is also used in organisations to reduce information systems diasters (Gotterbarn 2009). The IT Governance Institute (ITGI) states that effective ICT governance helps organisations ensure that their ICT can support business goals, maximise business investment in IT, and appropriately manage ICT-related risks and opportunities (ISACA 2007; Weill & Ross 2004a, 2004b).

Van Grembergen and De Haes (2008) assert that ICT governance is an integral part of corporate governance and is the responsibility of the governing body at a strategic level (e.g. the Board of Directors), management level (e.g. senior managers) and operational level (e.g. operational managers). On this account, at the strategic level, the responsibility of the board is to provide strategic alignment between business and ICT. At the management level, the responsibility of senior managers is to provide structures involving 'the organisation, and location of the ICT function, the existence of clearly defined roles and responsibilities and [a] diversity of ICT and business committees' (Van Grembergen & De Haes 2008, p. 24). At the operational level, control and monitoring processes for information systems need to be defined. Moreover, it is necessary that all three levels collaborate by establishing relational mechanisms such as 'business and ICT

participation, strategic dialogue, training, shared learning and proper communication' (Van Grembergen & De Haes 2008, p. 24).

Elieson (2006) argues that governance structure, defining responsibilities for managing risk, methodology, risk/process taxonomy, risk assessment, controls, transparency and business alignment are the key elements of an ICT risk framework. This implies that an ICT risk framework should be embedded in an organisation's ICT governance. Elieson (2006) adds that the risk framework should be mapped to ICT governance using a framework such as the Control Objectives for Information and related Technology (COBIT) framework. Because ICT governance provides guidance for the governing body to be responsible for ICT processes, those processes must be controlled and tested in an organisation's operational processes. In this regard, Posthumusa and Solms (2005, p. 12) claim that 'ICT governance is a continuous process, requiring ongoing review and adjustment and involves several concepts, including risk management, security, business continuity, change management, and regulatory compliance amongst several others'. Moreover, Tarantino (2008) asserts that strategic and operational risk can be managed by performing governance of risk management, which implies that ICT governance can occupy the role of ICT risk management within an organisation.

Korac-Kakabadse and Kakabadse (2001) argue that ICT governance focuses on the alignment of ICT objectives with business objectives in order to attain optimal business goals. In their view, ICT governance is a broad concept which consists of '(a) assessing the impact and nature of ICT, (b) the development of the IS/IT skill bases, (c) consideration of business, (d) legal and other IS/IT related issues, (e) the responsibility to safeguard the prime interests of all concerned—internal and external stakeholders, [and] (f) consideration of the structure and quality of the relationship among IS/IT stakeholders' (Korac-Kakabadse & Kakabadse 2001).

Two primary aspects of ICT governance are 'the value IT delivers to an organization and the control and mitigation of IT-related risks' (Hardy 2006, p. 56; Clementi & Carvalho 2007, p. 190). Hardy (2006) also notes that ICT governance should be a concern of organisational agendas and addressed by senior management in collaboration with the ICT department. According to Hardy, ICT governance encompasses five domains: (a) strategic alignment, (b) value delivery, (c) risk management, (d) resource management, and (e) performance measurement, where the first two are outcomes and the last three are drivers.

On the basis of the five areas of ICT governance outlined above, it can be argued that ICT governance in an organisation can streamline internal control processes and help an organisation achieve:

- ICT governance enhancement,

- improvement in understanding of ICT among executives,
- better decision-making with respect to quality and time frame allowed,
- alignment of ICT projects with business requirements,
- prevention of uncertainty around asset loss and systems breaches,
- compliance with regulatory requirements,
- competitive advantage through more efficient and effective operations,
- optimisation of operational processes with an integral part of security, availability, and information integrity, and
- enhancement of ICT risk management competencies and prioritisation of organisational ICT projects (Damianides 2005, pp. 81-82).

In relation to the benefits of adopting the ICT governance approach outlined above, Van Grembergen et al. (2004) argue that it can help an organisation define effective internal control processes regarding ICT governance structures and processes, roles and responsibilities, the ICT strategy committee, ICT steering committees, the ICT organisation structure, and strategic information systems planning. Clementi and Carvalho (2007) add that ICT governance covers two main criteria which organisations should consider: (a) strategic alignment that creates business value; and (b) risk management that maintains business value.

It can therefore be argued that ICT governance is the primary responsibility of executive management in terms of providing strategic direction on how to achieve business goals and objectives (Lainhart 2001b; Korac-Kakabadse & Kakabadse 2001; Bodnar 2003; Buckby et al. 2005); and one clear responsibility of executive management in ICT governance is risk management which is the main focus area of this research (Trites 2000, 2004; Buckby et al. 2005).

To simplify the ICT governance strategy, most organisations use an internationally recognised standard as a tool for creating and maintaining business value, such as the COBIT framework, the ISO/IEC 17799 standard or the Information Technology Infrastructure Library (ITIL) framework. However, this research focuses on ICT risk management planning by using the Control Objectives for Information and related Technology (COBIT) framework and the ISO/IEC 17799 standard because both are widely recognised and more concentrated on the internal organisational environment. One approach represents a top-down method while the other is essentially a bottom-up approach. Furthermore, the COBIT framework can help the researcher to define ICT

policy and ICT management processes for dealing with ICT risk management planning in an organisation. On the other hand, the ISO/IEC 17799 standard can supplement ICT risk management planning in terms of assisting with Information security policy, human resource management and information security management. Whether or not success factors based on the COBIT framework and the ISO/IEC 17799 standard affect the planning at both the corporate level and the operational level to establish this research outcome (i.e. successful ICT risk management) will be explored. The following section discusses the bottom-up approach.

2.4.2 Information security governance

The IT Governance Institute (2006b, p. 8) states that 'Information security governance is not only a technical issue, but [also] a business and governance challenge that involves adequate risk management, reporting and accountability'. The Institute also highlights that information security governance allocates the technical expertise for information security management to the ICT department (Solms 2005b). Information security governance is an integral part of corporate governance and must be aligned with the ICT governance framework and integrated into strategy, concept, design, implementation and operation in order to achieve effective corporate governance (Solms 2001).

The IT Governance Institute (2006b, p. 8) argues that the responsibility of executive management is to provide an overall information security strategy which includes:

- understanding of the information and information security that are critical to the organisation;
- reviewing investment in information security to ensure alignment of the organisation's strategy and risk profile; and
- endorsing the development and implementation of a comprehensive information security program.

Leadership, and organisational structures and processes, are the focus in information security governance, with the aim of helping the organisation develop relevant and effective processes to safeguard information (Solms 2001; ITGI 2006b). The IT Governance Institute (2006b, p. 13) states that the significant benefits of information security governance include:

- increased predictability and reduced uncertainty of business operations by lowering information security–related risk to a definable and acceptable level;

- assurance of effective information security policy and policy compliance; and
- a firm foundation for efficient and effective risk management, process improvement, and rapid incident response related to securing information.

Solms and Solms (2005, p. 272), and Solms (2006a, p. 166), argue that information security governance is a risk management or risk mitigation discipline. This is also argued in the following statement taken from *Information Security Governance: Guidance for the Board of Directors and Executive Management*: 'Information security programme is a risk mitigation method like other control and governance actions and should therefore clearly fit into overall enterprise governance'. Through a proper information security governance plan, the organisation must direct and control processes through the direction of the senior management, middle management and operational management levels.

Solms and Solms (2005, 2006) further argue that organisations must focus on directing and controlling processes to effectively manage ICT risk. Control processes are crucial at the strategic, tactical and operational levels responsible for ICT risks in an organisation. At the strategic level, senior management is responsible for providing the directives regarding both external factors (i.e. legal and regulatory prescriptions) and internal factors (i.e. the strategic vision, the role of ICT, alignment of ICT with company strategy and competitiveness). Likewise, senior management needs to ensure control compliance with the relevant directives. At a tactical level, middle management must follow the directives of senior management to expand sets of information security policies and ensure that the company's standards compliance and procedures are met. Furthermore, middle management should measure and monitor compliance with the requirements of the relevant policies, procedures and standards, and check their findings against their plan and that of senior management. At an operational level, the operational managers must ensure compliance with relevant administrative guidelines and procedures which reflect the prescribed operating procedures at all levels of the organisation. Operational management then controls a wide range of administrative guidelines and procedures including files about operating systems, databases, firewalls and other forms of utilities and specialised software sources. A summary of these management controls is presented in Table 2-3.

Table 2-3: A summary of the three different levels of management control

Level	Direct	Control
Strategic Level	- External factors - Internal factors	- The report reflecting compliance with relevant directives. - The report reflecting the relevant risk situations regarding information security.
Tactical Level	- Sets of relevant information security policies. - Sets of company standards and procedures.	- Measure and monitor the requirements at the strategic level. - Report on tactical level and report back to strategic level.
Operational Level	- Sets of relevant tactical documents are expanded by providing sets of administrative guidelines and administrative procedures to be followed at all levels.	- Log files of operating systems - Databases - Firewalls - Other forms of utility and specialised software sources.

Source: Adapted from Solms & Solms (2006)

In order to ensure that all relevant elements of information security governance are addressed in an organisational information security strategy, several security standards have been developed to provide guidance and ensure comprehensiveness. The most commonly and internationally used standard is the ISO/IEC 17799 standard as Information Security (IS) Governance (ITGI 2006b). The next section discusses the success factors of the COBIT framework.

2.5 Key factors in the COBIT framework: A top-down approach

2.5.1 Organisational policy

The Control Objectives for Information and related Technology (COBIT) is acknowledged internationally as the ICT governance standard. The COBIT framework is also recognised as a top-down or high-level framework for governance, security and control over ICT (Khan 2006; Smith & McKeen 2006). The COBIT framework helps organisations align business processes with ICT processes as well as manage ICT-associated risks (Lainhart 2001a). The COBIT framework provides good practice across a domain and process framework and presents activities in a manageable and logical structure.

Business control and technological control programs are the focus in the COBIT framework (Bae et al. 2003). ICT control is an integral part of the internal control of an organisation, which is a tool of corporate governance. The COBIT framework describes the information process requirements that match the broader classes of ICT control used by an organisation to achieve its objectives and goals. Internal control is viewed as a process in the COBIT framework which includes policies, procedures, practices and organisational structure that support the organisation achieving its goals and objectives (Colbert & Bowen 1996).

Robinson (2005) asserts that the COBIT framework stipulates that ICT processes and control should be aligned with business processes or aims. ICT processes and the control framework are derived from the attitudes, abilities, awareness and actions of the Board of Directors in relation to controls within an organisation. The COBIT framework was established as an ICT security and control practices standard to help senior management direct its responsibilities with regard to an organisation's assets by aligning the requirements in terms of business risk, control needs and technical issues (Bodnar 2006).

Moreover, the COBIT framework is used as high-level, detailed guidelines specifically in relation to information security (Solms 2005a). It has also been used as a primary standard to develop an Information Technology Risk Management System (ITRMS) at the University of Johannesburg (Solms 2006b). In this case, as Solm demonstrates, ICT risk governance is an integral part of corporate governance which is focused in some part on using the COBIT framework for ICT risk analysis.

The main purpose of the COBIT framework is to clarify business-focused, process-oriented, control-based and measurement-driven objectives and requirements by developing business processes and ICT systems in an organisation (ITGI 2007). In addition, as Solms (2005a), the ISM3 Consortium (2007) and Tshinu et al. (2008) all argue, the COBIT framework is an information security and management standard that classifies ICT processes and the control processes of what they do. However, Solms (2005a, p. 101) also claims that the COBIT framework is lacking in the area of information security control orientation, and does not detail 'how' information security control can be undertaken.

As illustrated in COBIT 4.1, the IT Governance Institute (ITGI) (2007), the business focus is business orientation which helps an organisation manage and control ICT resources. Moreover, a structured set of processes as outlined in the COBIT framework enables an organisation to ensure alignment to business requirements: 'Business requirements drive the investment in ICT resources that are used by ICT processes to deliver enterprise information which responds to business requirements' (ITGI 2007, p. 10).

2.5.2 ICT management

The process-oriented approach is presented in the COBIT framework as a reference process model that provides process details for everyone in an organisation to adopt in order to manage ICT activities and ICT risks. The COBIT framework includes four domains: '(1) Plan and Organize (PO)—Provides direction to solution delivery (AI) and service delivery (DS), (2) Acquire and Implement (AI)—Provides the solution and passes

them to be tuned into services, (3) Deliver and Support (DS)—Receives the solution and makes them usable for end users, (4) Monitor and Evaluate (ME)—Monitors all processes to ensure that the direction provided is followed.' The IT Governance Institute (2007, p. 12) model is shown in Figure 2-1.

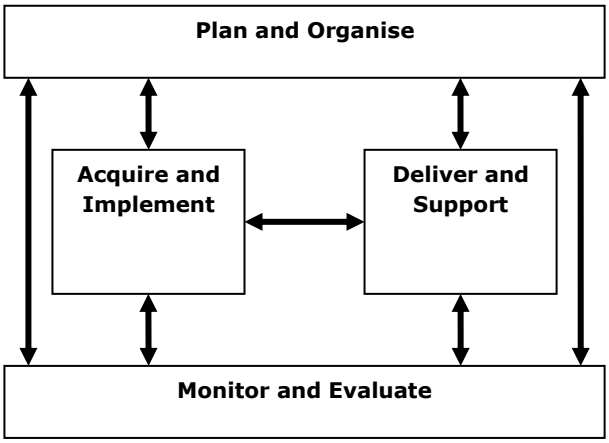


Figure 2-1: The four interrelated domains of the COBIT framework

Source: ITGI (2007, p. 12)

The four domains of the COBIT framework focus on the governing body and ICT management (Figure 2-1). This framework assists an organisation to build ICT processes and controls which are appropriate for implementing and developing ICT governance and management (Smith & McKeen 2006). The four domains consist of 34 processes and 210 control objectives that help an organisation define and follow its own approach to the management of ICT risks (ITGI 2007).

The plan and organise domain (PO): This domain provides ICT strategy and tactics that help ICT achieve the optimal contribution to the business objectives (ITGI 2007). The ITGI (2007) classifies this domain into 10 processes in combination with 74 control objectives that provide guidance on structuring an organisation. The ten processes are defined to ensure that business strategy, policies, procedures, processes and roles and responsibilities are determined by high-level management (ITGI 2007). In other words, people, process and organisational structure are all considered when planning how to deal with ICT risk.

The acquire and implement domain (AI): This domain allows for the realisation of ICT strategy based on the outcomes of the plan and organise domain to ensure that 'ICT solutions are identified, developed, acquired, implemented and integrated into the business processes', in turn to achieve business objectives (ITGI 2007, p. 13). The ITGI (2007) classifies this domain into seven processes in conjunction with 40 control objectives that provide guidance on maintaining and adapting existing organisational ICT systems. Seven processes are defined to assist in managing change, and whether the

existing system or a new system could best deliver ICT solutions to meet business objectives (ITGI 2007). The control objectives for this domain are aimed at ensuring that all ICT investment or new ICT projects are acquired to meet the needs of current business operations (ITGI 2007). In other words, the planning of ICT infrastructure and systems is considered necessary for dealing with ICT risks.

The deliver and support domain (DS): This domain enables the realisation of service activities such as the delivery of required services; security management and continuity; service support for users; data management and operational facilities in order to meet the requirements of day-to-day ICT operations (ITGI 2007). The ITGI (2007) defines this domain according to 13 processes along with 71 control objectives to ensure that ICT service activities serve ICT operations to meet business objectives. This domain implies that an organisation needs to consider which service activities best support ICT operations and control ICT processes to meet overall business operations.

The monitor and evaluate domain (ME): This domain raises awareness of ICT quality assurance required by an organisation to address performance management, monitoring of internal controls, regulations and governance (ITGI 2007). The ITGI (2007) categorises this domain into four processes along with 25 control objectives to ensure that: ICT performance is measured to detect problems before they occur; internal controls are effective and efficient; ICT performance can be linked back to business goals and can maintain confidentiality; and integrity and availability controls are considered in terms of information security.

Although there is a range of ICT control standards, frameworks and documents, the COBIT framework, as a model for ICT governance, is internationally recognised and applied widely in industry and commerce (Ridley et al. 2004; Buckby et al 2009). Elieson (2006) states that the COBIT framework is used as a baseline in ICT risk management to be mapped with other standards and frameworks to build a single, integrated body of work. The COBIT framework also includes a range of guidelines relevant to different areas of a framework including management guidelines, business function, control objectives, ICT governance implementation guidelines, control practices and ICT assurance guidelines (Lainhart 2001a; Ridley et al. 2004; ITGI 2007).

In terms of risk management, ICT processes and controls taken from the COBIT framework are focused on gaining control over risks. Therefore, all control objectives need to be discussed to determine which one is more applicable when dealing with specific ICT risks in an organisation. The high-level control objectives have been examined more in the practitioner research literature than in the academic research literature in relation to ICT control (Ridley et al. 2004; Liu & Ridley 2005; Gerke & Ridley 2006). According to studies by Guldentops et al. (2002), Huissoud (2005), Liu and Ridley

(2005), and Gerke and Ridley (2006), the most important control objective processes based on the COBIT framework (3rd and 4th versions) are the plan and organise; acquire and implement; and deliver and support domains. These findings are shown in Table 2-4.

Table 2-4: A comparison of the most important control objective processes within previous studies

ICT processes defined within the four domains based on the COBIT 3rd and 4th edition	Guldentops et al. 2002	Huissoud 2005	Liu and Ridley 2005	Gerke and Ridley 2006
Plan and organise domain				
PO1 Define a strategic IT plan	X	X	X	X
PO2 Define the information architecture		O		
PO3 Determine technological direction	X	O	X	
PO4 Define the IT processes, organisation and relationships				X
PO5 Manage the IT investment	X		X	X
PO6 Communicate management aims and direction				X
PO7 Manage human resources				
PO8 Ensure compliance with external requirements				X
PO9 Assess risks	X	O	X	X
PO10 Manage projects	X	O		
PO11 Manage quality			X	
Acquire and implement domain				
AI1 Identify automated solutions	X	O	X	
AI2 Acquire and maintain application software	X	O	X	X
AI3 Acquire and maintain technology infrastructure		X		X
AI4 Develop and maintain procedures		O		
AI5 Install and accredit systems	X		X	X
AI6 Manage changes	X	X	X	X
Deliver and support domain				
DS1 Define and manage service levels	X		X	
DS2 Manage third-party services				
DS3 Manage performance and capacity				
DS4 Ensure continuous services	X	X	X	X
DS5 Ensure system security	X	X	X	X
DS6 Identify and allocate costs				
DS7 Educate and train users		X		
DS8 Assist and advise customers				X
DS9 Manage the configuration				X
DS10 Manage problems and incidents	X	X	X	X
DS11 Manage data	X	O	X	X
DS12 Manage facilities				X
DS13 Manage operations				
Monitor domain				
M1 Monitor the processes	X	X	X	
M2 Assess internal control adequacy				
M3 Obtain independent assurance				
M4 Provide for independent audit				
Legend X = Most important O = Also important				

Source: Adapted from the studies of Guldentops et al. (2002); Huissoud (2005); Liu & Ridley (2005); Gerke & Ridley (2006)

Previously researchers have identified that the most important control objective processes are in the PO, AI, and DS domains for ICT control. The least important domain is the monitor domain because the research indicates that organisations are concerned with only M1 ('monitor the processes') in the monitor domain. However, prioritising the control objective process in organisations does not differ depending on a change in ICT situation or type of industry or sector (Guldentops et al. 2002; Ridley et al. 2004; Liu & Ridley 2005; Gerke & Ridley 2006). Furthermore, these four studies have concluded that PO1 (Define a strategic ICT plan), AI6 (Manage change), DS4 (Ensure continuous service), DS5 (Ensure system security) and DS10 (Manage problems and incidents) appear to be the most important elements to be considered in an organisation. This implies that ICT strategies, change management, business continuity planning, and security and risk management have been found in these studies to be the most critical to be defined in order to prevent, mitigate and avoid ICT risk. However, as the COBIT framework has some limitations, it is more concerned with ICT governance and management than information security (IS) governance and management. It can therefore be seen that IS governance and management can fill this gap by providing the controls for IS strategies, business continuity, change management, and risk management in security planning (ITGI 2006b; ISO/IEC 2005). The next section discusses the success factors of the ISO/IEC 17799 standard.

2.6 Key factors in the ISO/IEC 17799 standard: A bottom-up approach

2.6.1 Organisational policy

The major aim of the ISO/IEC 17799 standard is to emphasise internal control through policies, procedures and risk assessment (Capuder 2004). This differs from the COBIT framework in that the ISO/IEC 17799 standard provides the details of organisational information security practices rather than focusing on ICT controls. Moreover, the ISO/IEC 17799 standard is used more as a low-level guideline that details the specifics of 'how' information security should be done (Solms 2005a). Solms (2005a) also mentions that the ISO/IEC 17799 standard focuses on technological orientation in terms of providing guidance on precisely 'how' control objectives can be achieved. On the other hand, the COBIT framework focuses on business orientation which describes the control objectives at the higher level, by describing 'what' control objectives need to be considered.

Therefore, this study argues for selecting the merits of both the framework and the standard to create a single management framework for dealing with ICT risk management planning in an organisation. Moreover, in this regard the COBIT framework

itself stipulates that its framework can complement other standards and frameworks (ITGI 2007), although there is no research that proposes how they can fit together in the context of a structured approach to ICT risk management (Tshinu et al. 2008; Siponen & Willison 2009).

2.6.2 Information security management and human resource management

The ISO/IEC 17799 standard defines information security as a crucial area that all employees of an organisation must master in order to ensure business continuity, mitigate business risk and maximise returns on investment and business opportunities (Groves 2003). Myler and Broadbent (2006) and Groves (2003) assert that the ISO/IEC 17799 standard is a detailed security standard which is organised into several information security management practices, including:

- creating an information security policy guideline;
- assigning information security roles and responsibilities;
- providing consistent asset management;
- establishing human and physical security mechanisms;
- reporting security incidents and business continuity management;
- determining access control and associated systems;
- documenting communication and operational procedures; and
- complying with legal requirements and audit controls.

Myler and Broadbent (2006) also state that the ISO/IEC 17799 standard is a framework for establishing risk assessment methods including policies, control, countermeasures and program documentation. Moreover, a basic requirement of the ISO/IEC 17799 standard is security risk analysis which is referenced throughout the standard, and various resources are available to assist with this (ISO/IEC 17799 Compliance Associates 2002). The relationship between risk analysis and compliance with ISO/IEC 17799 is very close. It is therefore important to ensure that the methodology adopted is fully consistent with the demands of the standard. Haworth and Pietron (2006) articulate that ISO/IEC 17799 can be used as an ICT control and audit framework.

Eloff and Eloff (2003) point out that the ISO/IEC 17799 standard is used to act as an information security management system to allow an organisation to initially concentrate on specific security sections. This standard also expands ICT orientation to address both

ICT and security orientations when dealing with ICT risk management in an organisation (Eloff & Eloff 2003).

The ISO/IEC 17799 standard provides the most comprehensive approach to information security management which can streamline ICT governance of the technical aspects of information security (Saint-Germain 2005). It also helps execute a cost-effective plan which includes appropriate security controls in order to mitigate risks and protect the confidentiality, integrity and availability of information assets in an organisation (Saint-Germain 2005; Theoharidou et al. 2005). Moreover, the ISO/IEC 17799 standard defines that information security management is part of ICT risk management as a process of identifying, controlling, and minimising or eliminating security risks that may affect information systems, at an acceptable cost (ISO/IEC 2005).

Two main aspects of information asset protection in ISO/IEC 17799 emphasise information security and information system security (Theoharidou et al. 2005). Information security refers to the safeguarding of information integrity—that is, confidentiality, integrity and availability. Information system security refers to the protection of all information system elements such as hardware, software, peopleware, information and processes. Theoharidou et al. (2005) reveal that most organisations select appropriate control objectives to deal with insider threats which are based on implementation of the ISO/IEC 17799 standard. In dealing with insider threats, the personal security category is selected to determine the management of job descriptions of security staff; personnel screening; confidentiality agreements; security responsibility in the terms and condition of employment; and information security and training (Theoharidou et al. 2005).

The ISO/IEC 17799 provides the specific guidance needed for an organisation to establish information security management (Sweren 2006). This specific guidance consists of information security process; information security roles and responsibilities; and any relevant regulations. The ISO/IEC 17799 standard has been renamed according to the new numbering scheme in 2007 as the ISO/IEC27000 series (Broderick 2006; Sweren 2006); however, the content is identical in the two standards.

A study conducted by Karabacak and Sogukpinar (2006) utilising a quantitative method for the ISO/IEC 17799 standard gap analysis involved measuring 133 control objectives grouped into 11 domains of the ISO/IEC 17799 in order to gain accurate compliance results. The number of questions aligned with the 133 control objectives regarding information security management. However, the number of questions can be less than or equal to the number of control objectives in the standard depending on the organisational structures and processes within the organisation. The results of their research indicated which domains are more compliant to the standard. More compliance

in the standard is concerned with the areas of organisational rules and regulations; security policy; human resources security; and information security acquisition, development and maintenance. Furthermore, each domain is concerned with different staff level perspectives. For example, senior management is concerned with some domains in the standards such as security policy, the organisation of information security, human resources security, business continuity management and compliance.

A study by Gordon et al. (2006) investigated the voluntary disclosure of information security activities in US corporations as reported to the Security and Exchange Commission (SEC) between 2000 and 2004 (five years of the annual filing data). Their report illustrated that 24 key words (refer to Table 2-5) commonly appeared in 27,253 annual reports of US corporations which are repeatedly reported to the SEC (Gordon et al. 2006).

Table 2-5: Listing of key words used for disclosure search

Key word	Number of instances	Categories of disclosure
Security measure	2,211	1
Authentication	1,823	
Encryption	1,411	
Disaster recovery	1,182	
Information security	937	
Access control	595	
Business continuity	406	
Security management	224	
Security monitoring	188	
Cyber security	26	
Infosec	7	
Security expenditure	7	
Computer system security	3	
Cyber security	3	
(Network or computer) join (1) security	906	2
Hacker	204	
Denial of service	158	
Cyber attack	19	
Computer virus	1,277	3
Security breach	1,209	
Intrusion	573	
Security incident	16	
Computer breach	2	
Computer intrusion	1	
Total instances	13,388	
Categories: (1) disclosure of proactive steps toward improving information security, (2) disclosure of information security vulnerabilities, and (3) disclosure of information security breaches.		

Source: Adapted from Gordon et al. (2006)

In US corporations, information security management involves proactive steps toward improving information security. Moreover, the findings in Gordon et al.'s (2006) research suggest that information security management must be planned in advance in order to prevent, avoid and mitigate information security vulnerabilities and information security breaches. Gordon et al. (2006) also conclude that securing the information environment appears to be gaining increased attention in organisations. It is imperative that the ISO/IEC 17799 standard is taken into account because all these concerns are covered in the detailed processes of the ISO/IEC 17799 standard as opposed to the COBIT framework. However, considering the ISO/IEC 17799 standard alone is not adequate because its approach to ICT management does not cover ICT resources or governance of ICT organisational structure, policies and strategies. Therefore, the two-way approach works well as the COBIT framework lays the foundation for ICT governance and management (e.g. the top-down approach) to risk management, while the ISO/IEC 17799 standard focuses on IS governance and management (e.g. the bottom-up approach) to risk management.

2.7 The management level plan vs. the operational level plan in ICT risk management

The COBIT framework provides general management guidelines for assisting organisations to manipulate ICT assets and facilitate ICT processes to ensure effective ICT risk management (Bodnar 2006). It categorises critical success factors that can be applied in an organisation's processes such as 'processes and policies description, clear duty and task, management commitment, appropriate communication to concerned internal and external persons and consistent measurement practices' (Hawkins et al. 2003). It is widely recognised as one of the most effective tools in ICT governance for ICT risk management (Khan 2006).

The ISO/IEC 17799 standard consists of 124 control objectives categorised into 10 ICT audit and control areas based on ISO/IEC 17799. However, the new version of the ISO/IEC 17799 standard, revised in 2005, includes 133 controls in 11 different domains. It addresses 11 areas: 'security policy, organization of information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, information systems acquisition, development and maintenance, information security incident management, business continuity management and compliance' (Broderick 2006, p. 27; Karabacak & Sogukpinar 2006, p. 416; Sweren 2006). To propose aligning this standard with the COBIT framework, these 11 domains are summarised in conjunction with the four domains of the COBIT framework in Figure 2-2.

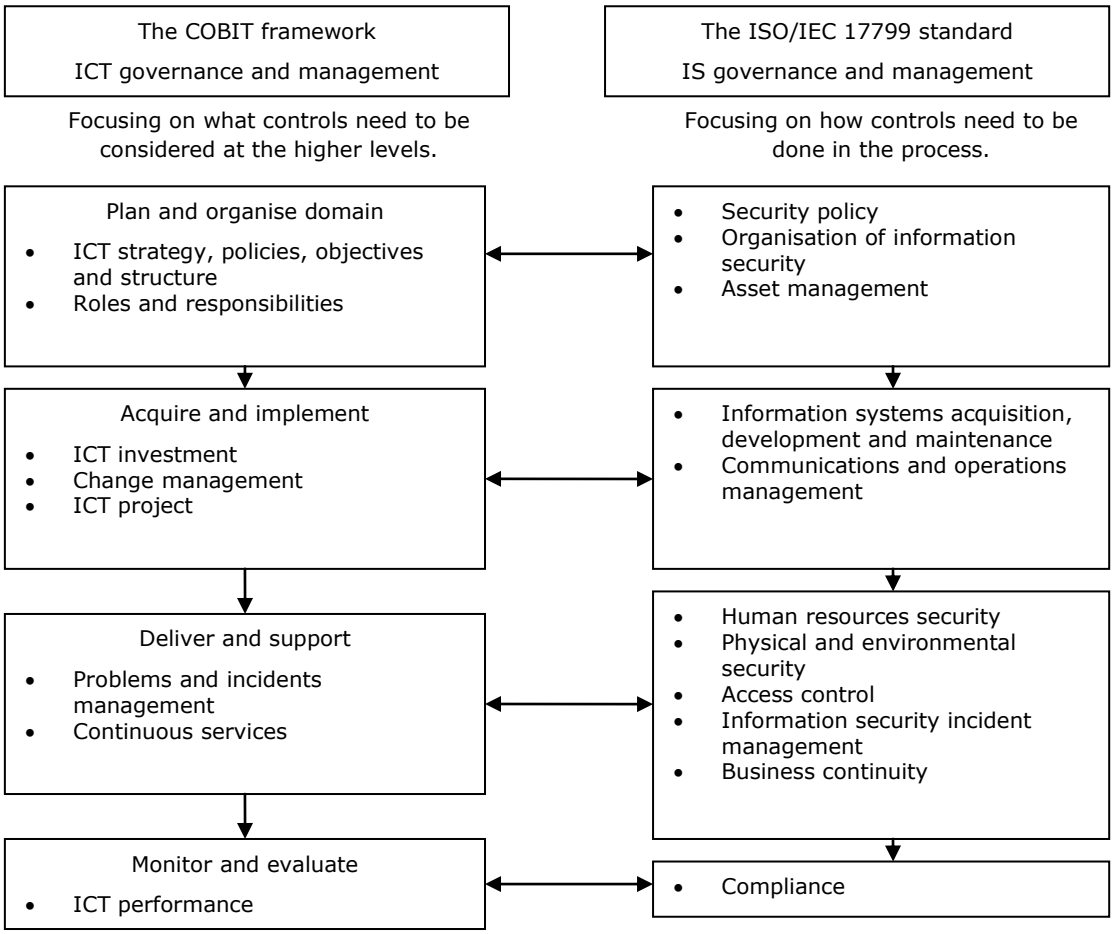


Figure 2-2: Mapping the ISO/IEC 17799 standard with the COBIT framework

Source: Adapted from ITGI/OGC (2005), ITGI (2006a), ISO/IEC (2005) and Broderick (2006)

The mapping in Figure 2-2 reveals that the COBIT framework is used to align with business orientation. In contrast, the ISO/IEC 17799 standard is used to align with ICT orientation. Therefore, integrating the COBIT framework and the ISO/IEC 17799 standard into one single management framework for ICT risk management will enable a focus on alignment of business, ICT and security orientations simultaneously. The mapping above shows that the ISO/IEC 17799 standard supplements the COBIT framework in each part of each domain in security-related matters, which can effectively strengthen ICT strategy through IS strategy to meet business objectives when dealing with ICT risks.

A number of research projects have been carried out with respect to the effectiveness of the COBIT framework in ICT risk management. For example, Solms (2005a) shows that the COBIT framework is a high-level control objective framework which is a superior ICT governance framework. It provides detailed instructions on 'what' must be done in an organisation with respect to ICT risk management. Lainhart (2001b) demonstrates that the COBIT framework occupies the primary role in overall business control.

The COBIT framework, however, is less detailed on the technical side of 'how' this should be undertaken (Solms 2005a). To address this issue the ISO/IEC 17799 standard is

presented to complement the COBIT framework. The ISO/IEC 17799 standard ensures that a technical perspective is taken into account at the management level in order to streamline management processes and procedures as outlined in annual planning (Eloff & Eloff 2003). It is aimed at providing organisations with a holistic technical approach which includes technical specifications such as network systems security, personnel security and organisational security (Kenning 2001; Theoharidou et al. 2005).

Buchanan and Gibb (2007) assert that the role and scope of the information audit used in an organisation are often neglected or forgotten in our understanding of processes and practice. There are three main problems related to the information audit: 'Firstly, the top-down approach itself still has a lack of clear top-down strategic direction. Secondly, there is less practical guidance on the scope of the information audit. Thirdly, there is no standard, agreed methodological approach to information audit' (Buchanan & Gibb 2007, p. 3). It can thus be argued that the information audit and control lack clarity in terms of their scope and roles with regard to ICT risk management.

Much research has been conducted on the use of the ISO/IEC 17799 standard for effective ICT risk management. For example, Groves (2003) demonstrates that the ISO/IEC 17799 standard provides more technical orientation in relation to ICT risk management, such as generating a document of information security policy; assigning responsibility for information security; training and educating about information security; reporting security incidents; and establishing a plan of business continuity management. Moreover, the process of protecting information entails a collaborative effort among all employees in an organisation. Capuder (2004) concludes that all levels of an organisation must commit to the processes which deal with information security. The ISO/IEC 17799 standard includes direction for technical staff such as auditors or security professionals, requiring them to deal with information security. Theoharidou et al. (2005) show that using the ISO/IEC 17799 helps organisations handle computer abuse from insider threats—that is, threats derived from employees who have authority access to IS and misuse its objective—by focusing on personnel security.

Both the COBIT framework and the ISO/IEC 17799 standard recognise two aspects of information security in ICT governance when dealing with ICT risk management: business orientation and technical orientation. To better understand these two frameworks, a comparative analysis of their differences in terms of business orientation and technical orientation is clearly desirable. Table 2-6 presents the results of this comparison (Lientz & Larssen 2004, 2006).

Table 2-6: A comparison between business, information and communication technology and information security orientations in ICT risk management

Focus	Business	Information and Communication Technology (ICT)	Information Security (IS)
Governance	- Corporate governance	- ICT governance and management	- IS governance and management
Nature of work	- Business transactions	- ICT transactions	- Security transactions
Concentration	- Business objectives - Business strategies - Business policies - Business goals - Business processes	- ICT objectives - ICT strategies - ICT policies - ICT goals - ICT processes	- IS objectives - IS strategies - IS policies - IS goals - IS processes
Activity	- Business control and audit	- ICT control and audit	- IS control and audit
Approach	- Top-down - Bottom-up - Two-way	- Top-down (the main responsibilities lie with high-level management)	- Bottom-up (the main concern is on processes)
Alignment	- ICT and IS	- Business	- ICT and business
Management	- Business risks regarding strategies, policies and operations	- ICT risks regarding ICT strategies, ICT policies and ICT operations	- Security risks regarding IS strategies, IS policies and IS operations

Adapted from Lientz & Larssen (2006)

From the data outlined in Table 2-6, it can be concluded that governance in an organisation should focus on ICT and IS aligning with business when dealing with ICT risk management. When only one perspective is the focus, the relevance of ICT control and audit may not be found when dealing with ICT risks. It is recommended that ICT and IS perspectives be considered such that they supplement each other to align with the business perspective (ITGI 2007). In this regard, this research takes this opportunity to empirically explore and explain the phenomenon by using both perspectives to deal with ICT risk management.

Jordan and Silcock (2005) suggest that ICT risk management should adopt both top-down and bottom-up approaches. Such an integration of the COBIT framework and the ISO/IEC 17799 framework can be used to streamline business needs by focusing on four key elements in organisational ICT risk management: strategy and policy; roles and responsibilities; processes and approach; and people and performance (Jordan & Silcock 2005; Robinson 2005). Mena (2002) demonstrates that the close cooperation between senior management and the operational team can lead an organisation to attain the optimal goals in ICT risk management. Table 2-6 reveals that the common goals of an organisation are to plan and organise ICT risk management from business, ICT and IS perspectives based on internal control regarding corporate governance, ICT governance and IS governance.

Focusing solely on an ICT perspective may lead to a reduced emphasis within corporate governance on risk management, especially related to ICT. ICT governance is the responsibility of senior management to provide strategic direction for technological

operations in order to achieve business goals and objectives (Bodnar 2003; Buckby et al. 2005; ISACA 2007; ITGI 2007; Korac-Kakabadse & Kakabadse 2001; Lainhart 2001a; Ridley et al. 2004; Smith & McKeen 2006). One clear responsibility of executive management in ICT governance is ICT risk management (Buckby et al. 2005; Trites 2000; 2004). IS governance is specifically used to align with the ICT governance framework as an integrated strategy in order to achieve effective corporate governance (Solms 2001). Information security (IS) governance focuses on leadership, organisational structures, and processes to help the organisation provide relevant and effective processes to safeguard information (Solms 2001). Significantly, its benefits lead to '(a) increased predictability and reduced uncertainty of business operation by lowering information security–related risk to a definable and acceptable level, (b) assurance of effective information security policy and policy compliance, and (c) a firm foundation for efficient and effective risk management, process improvement, and rapid incident response related to securing information' (ITGI 2006b, p. 14).

2.8 Key factors for ICT risk management success

The research literature has shown that ICT risk management focuses on three main components: ICT risk management process, ICT risk management control and ICT risk management planning. ICT risk management process and control are considered to manage ICT risks in the area of human resource management, ICT management and IS management. By doing so, an organisation can successfully avoid, mitigate and prevent ICT risks. However, the nature of ICT risk management planning varies or is ill-defined because there is little common understanding, or agreed upon formula, for academics and practitioners to follow. Therefore, this research uses a structured approach to conceptualise the guidance for ICT risk management; and this structured approach is based on integration of the COBIT framework and the ISO/IEC 17799 standard.

According to the above discussion on the COBIT framework and the ISO/IEC 17799 standard, this chapter has highlighted the success factors for ICT risk management. Five key factors (information and communication technology policy, information security policy, ICT management, information security management and human resource management) derived from the COBIT framework and the ISO/IEC 17799 standard affect planning at the management level and the operational level around successful ICT risk management. Each key factor is discussed below.

Firstly, information and communication technology policy focuses on ICT strategy that relates to the direction of ICT control and audit. With the direction of ICT control and audit, an organisation must pay attention to the alignment of ICT processes with

business orientation. Moreover, an organisation must clarify what kind of ICT process and control can help achieve organisational goals and objectives for dealing with ICT risks.

Secondly, information security policy focuses on information security (IS) strategy relating to the direction of IS control and audit. With this direction, an organisation seeks to control ICT infrastructure and systems by using information security processes to align with ICT processes. In addition, Information security policy supports IS processes to attain greater sophistication in technical areas. This policy also helps determine how control objectives can develop the right technical orientation for securing information and information assets.

Thirdly, ICT management is another key factor that an organisation seeks to provide the view of management in ICT activities. ICT activities penetrate the organisational structure and business transactions of modern businesses. Therefore, ICT management helps an organisation manage ICT infrastructure in both ICT implementation and development.

Fourthly, information security management is used to manage security incidents in ICT systems. It is also used to maintain the confidentiality, integrity and availability of information assets in modern organisations. Information security management mainly focuses on the protection of all information system elements such as hardware, software, information and processes.

Fifthly, human resource management is also considered in terms of the protection of people and their behaviour in an organisation that is relevant to all ICT systems. In a modern organisation, human resources are the key organisational asset involved in the setting of organisational policy, the control of ICT processes and the management of information assets. Therefore, all staff levels are required to be managed and controlled in a proper manner in order to achieve all organisational requirements.

These five key factors have the main impact on planning at both the management and operational levels. In general, the manager is the key person to set the overview plan (i.e. the management plan or the corporate plan) for ICT risk management. The overview plan initially defines what ICT processes need to be adopted to prevent, avoid and mitigate ICT risk. From there, the plan is implemented at the operations level in order to help individual departments set their own plans (i.e. the operational plan or the action plan) for dealing with ICT risk.

Both the COBIT framework and the ISO/IEC 17799 standard are followed to help an organisation facilitate the setting of ICT risk management planning. The COBIT framework assists with the development of ICT policy and management which impact on planning around ICT risk management at the corporate level. On the other hand, the

ISO/IEC 17799 standard helps with the setting of Information security policy, IS management and human resource management which affect planning around ICT risk management at the operational level. In terms of successful ICT risk management, academics and practitioners argue that ICT risk must be mitigated, avoided and prevented in order to ensure that the business goals and objectives can be met.

Table 2-7: A summary of key factors of successful ICT risk management in previous research, in the COBIT framework and in the ISO/IEC 17799 standard

Research Literature	The COBIT framework (focused on at the highest appropriate organisational level)	The ISO/IEC 17799 standard (focused on at the operational level)
Relevant policy in place (Benaroch et al 2006; Buckby et al. 2009; Capuder 2004; Cha et al. 2008; Colbert & Bowen 1996; Fletcher 2006; Gallegos et al. 2004; Khan 2006; MyEvoy & Whitcombe 2002; Segars & Grover 1996; Smith & McKeen 2006; Solms 2005a)	Creating ICT policy to define a strategic ICT plan and to determine technological direction	Creating information security policy to document information security policy and to review of the information security policy.
Policy and mechanisms in place to protect ICT resources such as information assets, ICT infrastructures and ICT architecture (Benaroach et al 2006; Bodnar 2006; Buckby et al. 2009; Byrd et al. 1995; Fletcher 2006; Longstaff et al. 2000; Smith & Eloff 2002; Stoneburner et al. 2002; Straub & Welke 1998)	Effective ICT resource management with regard to ICT infrastructure, ICT performance, ICT project,	Not clearly defined
Policy and mechanisms in place to manage human resources and defining roles and responsibilities (Badenhorst & Eloff 1994; Ciborra 2006; Figg 1999; Hughes 2006a; Moulton 2003; Van Grembergen & De Haes 2008; Willcocks & Griffiths 1994; Willcocks et al. 2006)	Constant management of human resource including training and educating programs.	Constant human resource security for employees during employment and termination or change of employment
Policy and mechanisms in place to manage access control in physical and logical systems (Badenhorst & Eloff 1994; Hayat et al 2007; Levine 2004; Milenkovic 2008; Schultz 2007)	Creating a process for managing the physical environment	Creating a process for secure areas, equipment security, user access management, user responsibilities, network access control, operating system access control and application and information access control.
Policy and mechanisms in place to manage business continuity planning (Cha et al. 2008; Groves	Creating a continuous services plan	Creating business continuity management and information security incident planning and management

2003; ISO/IEC 2005; ITGI 2007; Posthumusa & Solms 2005)		
Implementation of control mechanisms to secure information, information systems and assets (Bodnar 2006; Byrd et al. 1995; Karabacak & Sogukpinar 2006; Lainhart 2001a; Longstaff et al. 2000; Smith & Eloff 2002; Stoneburner et al 2002)	Implementation of an ICT plan (e.g. defining ICT processes) regarding the ICT infrastructure and for developing of a security culture	Implementation of the organisation of information security and asset management to create an ICT security plan (e.g. defining information security processes)
Implementation of control mechanisms to protect information integrity such as input, processing and output (IPO) processes (Bojanc & Jerman-Blazic 2008; Coles & Moulton 2003; Flowerday & Solms 2005; Hermanson et al 2000; Moeller 2005; Saint-Germain 2005; Smith & Eloff 2002; Theoharidou et al. 2005)	Implementation of ICT processes, technology infrastructure, and data management	Implementation of information systems development and maintenance
Implementation of control mechanisms to protect threats and vulnerabilities of assets (Anderson & Choobineh 2008; Hawkins et al. 2003; Karabacak & Sogukpinar 2006; Ksiezopoliski & Kotulski 2007; Smith & Eloff 2002)	Not clearly defined	Implementation of organisation of information security; internal organisation focusing on vulnerability of assets and external environment focusing on threats.
Operationalisation of ICT management control (Elieson 2006; Eloff & Eloff 2003; Finne 2000; Flowerday & Solms 2005; Gerke & Ridley 2006; Khan 2006; Liu & Ridley 2005; Ridley et al. 2004; Robinson 2005; Smith & Eloff 2002; Smith & McKeen 2006; Van Grembergen et al. 2004)	Implementation of ICT processes to control ICT management	Not clearly defined
Operationalisation of information security control (Capuder 2004; Eloff & Eloff 2003; Fletcher 2006; Flowerday & Solms 2005; Hayat et al. 2007; Kenning 2001; Khan 2006; Robinson 2005; Smith & McKeen 2006; Solms & Solms 2005, 2006; Solms 2005a; Straub et al. 2008)	Not clearly defined	Implementation of information security processes to control information security management

The results of a comparison between the research literature on the COBIT framework and on the ISO/IEC 17799 standard are shown in Table 2-7.

2.9 Conclusion

ICT risk management is primarily the remit of senior management. Nonetheless, some researchers argue that senior management often avoids concerning itself with ICT security (Byrd et al. 1995), which may lead to a lack of technical planning in ICT risk management. This research uses the COBIT framework and the 17799 standard to bridge this gap. As a result, this study argues for selecting the merits from both the framework and the standard to create a single management framework for dealing with ICT risk management planning in an organisation. The analysis in this chapter is used in the initial part of this research to understand the phenomenon of ICT risk management planning in Thai organisations. By doing so, this research firstly investigates the current ICT risk management practices in Thai organisations, and then, secondly, identifies the success factors for effective ICT risk management. The aim is to develop a single management framework for successful ICT risk management planning by building a research framework for testing. The next chapter discusses the research method and research design used to build and test success factors of ICT risk management.

Chapter 3

RESEARCH METHODOLOGY

This chapter discusses the research methods employed in this study. The chapter is structured as follows: the first section highlights the research paradigm; section two discusses the research methods; section three outlines the data collection and data analysis methods; and the last section covers the research design, summary and conclusion.

3.1 Research paradigm

A research paradigm is an underlying philosophical approach taken to research. This section describes the meanings of the two research methods used in this research and concludes with a discussion of the pragmatist approach selected for the current study.

According to Neuman (2006, pp. 81-82), 'modern positivism founded by Auguste Comte (1798–1857) adopts an essentialist orientation to reality: Reality is real; it exists "out there" and is waiting to be discovered'. This implies that the positivist approach allows the researcher to verify the theoretical interest (i.e. opinions, ideas and conceptual model) to be validated as a true model or concept (Lee 1991). In contrast, Lee (1991, p. 347) argues that 'passing an empirical test can never verify conclusively that the theory of interest is true'. This argument is augmented by the view that 'it should be noted that a positive decision can only temporarily support the theory, for subsequent negative decisions may always overthrow it [Popper 1968, p. 33]' (Lee 1991, p. 347). In this regard, one imperative approach, the interpretive approach (founded by Max Weber 1864–1920), has been proposed to resolve the problem outlined above (Lee 1991; Neuman 2006). An interpretive approach allows the researcher to understand 'social construction and meaning rather than only social structure and social facts [King 1996]' (Silverman 1998, p. 5).

With a view to taking advantage of both the positivist and interpretivist approaches, this research uses a mixed-methods approach that incorporates the intention to shape the

theoretical knowledge of ICT risk management in an organisation. Qualitative research is seen as helping the researcher to explore the practice of ICT risk management in an organisation. On the other hand, the quantitative research method enables the researcher to explore the relationships between success factors in the phenomenon of ICT risk management in an organisation in practice. This research was guided by the work of Creswell and Plano Clark (2007), Lee (1991), Neuman (2006), Silverman (1998) and Tashakkori and Teddlie (2003) with the aim of synchronising and utilising both the qualitative and quantitative approaches to investigate ICT risk management through the lens of pragmatism (Peirce [1839–1914], James [1842–1910], Dewey [1859–1952], and Mead [1863–1931]) (Baert 2005). Pragmatism allows the researcher to use mixed-methods research such as paradigm pluralism (Creswell & Plano Clark 2007; Tashakkori & Teddlie 2003) and thereby to answer the research questions through a series of research methods.

3.2 Research method

Mixed-methods research is powerful and elucidates 'quantitative and qualitative research methods focused on the philosophical assumption and methods of inquiry' (Creswell & Plano Clark 2007, p. 5). Neuman (2006) argues that quantitative and qualitative research methods supplement each other, although they are different in terms of research design, data collection and data analysis.

Todd et al. (2004, p.1) argue that quantitative and qualitative research methods compete with each other in regard to 'philosophical and theoretical issues'. However, they are suitable for different rationales and thus researchers could feasibly ignore these particular issues in taking advantage of both approaches (Todd et al. 2004). Research methods based on quantitative and qualitative research can be understood in terms of the involvement of the researcher in the research, which Todd et al. (2004, p. 4) have described as 'reflexivity'.

Tashakkori and Teddlie (2003) [cited in Erzberger & Prein 1997] argue that the quantitative research method cannot be carried out in the initial phases of social research as exploratory research is different from the qualitative research method. This implies that the quantitative research method is restricted in terms of its use in social research. The difference between quantitative and qualitative research depends upon the direction and procedure of data collection and analysis (Creswell & Plano Clark 2007; Neuman 2006; Tashakkori & Teddlie 2003).

For example, with quantitative research the action of the researcher in the process of data collection is detached from the research being investigated as 'object (the

investigated)' (Neuman 2006; Todd et al. 2004, p. 4). In contrast, qualitative research involves the researcher getting involved in the data collection to construct the project as 'subject (investigator)' (Neuman 2006; Todd et al. 2004, p. 4).

Mixed-methods research is characterised by the collection of both qualitative and quantitative data and analysed sequentially or concurrently in one research project (Creswell & Plano Clark 2007); thus one research project provides sequential or concurrent data collection and then also conducts two different data analysis methods. Furthermore, each research method can enrich the findings of the other (Hanson et al. 2005; Brewer & Hunter 1989; Tashsakkori & Teddlie 2003). For example, one method is used to collect qualitative data to explore and understand the central phenomenon represented in the qualitative results (Gable 1994). The findings from that research are then used to shape the instrument used in the quantitative data collection in order to confirm and validate the original research findings through the quantitative analysis (Gable 1994).

Hanson et al. (2005, p. 226), Mertens (2003) and Punch (1998) suggest that 'mixed methods investigations may be used to (a) better understand a research problem by converging numeric trends from quantitative data and specific details from qualitative data; (b) identify variables/constructs that may be measured subsequently through the use of existing instruments or the development of new ones; (c) obtain statistical, quantitative data and results from a sample of a population and use them to identify individuals who may expand on the results through qualitative data and results; and (d) convey the needs of individuals or groups of individuals who are marginalized or underrepresented'. Thus, the key benefit of mixed-method research is that both the qualitative and quantitative method can be used to elaborate on the results from one part of the research, to help the researcher develop the other part (Hanson et al. 2005).

Plano Clark et al. (2008, p. 1546) argue that 'broadly speaking, mixed methods research refers to the combination of quantitative research and qualitative research [Greene et al. 1989] and its basic premise is that the combination provides a better understanding of research problems than either approach by itself [Creswell 2005]'. In addition, Tashakkori and Teddlie (2003, p. 15) claim that 'mixed methods research enables the researcher to simultaneously answer confirmatory and exploratory questions, and therefore verify and generate theory in the same study'. Consequently, this research uses a mixed-methods approach as the most effective means to explore, understand and confirm success factors of ICT risk management in Thai organisations.

3.2.1 Quantitative research method

The quantitative research method is largely based on the positivist paradigm used within social science (Neuman 2006). It is applied to define a set of relationships, variables and/or hypotheses for validating and confirming the quantitative findings (Neuman 2006). Furthermore, the quantitative research method is associated with '(a) inferential statistics; (b) hypothesis testing; (c) mathematical analysis; (d) and experimental and quasi-experimental design' (Lee 1991, p. 342; Kaplan & Duchon 1988).

This method is also used to generate and verify existing research and theory (Tashakkori & Teddlie 2003). Quantitative data collection is relevant to dealing with a large sample size in order to generalise the findings to formulate ideas, concepts, frameworks and theory. Quantitative data analysis typically uses statistics and statistical analysis to test hypotheses (Kaplan & Duchon 1988).

The quantitative research method primarily helps the researcher to test continual hypotheses rather than to build theory, according to Kaplan and Duchon (1988) citing Glaser and Strauss (1967). This is important as the main purpose of this research is to build theory on the subject of ICT risk management in organisations. According to Kaplan and Duchon (1988), using the quantitative research method alone does not enable researchers to construct theory. Therefore, it is imperative to take the qualitative research method into consideration also.

3.2.2 Qualitative research method

The qualitative research method relies on the interpretivist paradigm within social science (Neuman 2006). It is normally used to 'understand and explain social phenomena' (Myers 1997, p. 1). Walsham (2006, p. 320) argues that the interpretive research method includes 'the domain of human action, [which] is a social construction by human actors'. This implies that through this method a researcher attempts to understand, conceptualise and construe the meaning of the phenomenon of a particular subject or circumstance (Kaplan & Duchon 1988). Furthermore, interpretation of human action is related to 'ethnography, hermeneutics, phenomenology and case studies' (Lee 1991, p. 342).

The nature of the interpretive research method is to focus on 'human thought and action in the social and organizational context' (Klein & Myers 1999, p. 67) by using different data collection and analysis methods taken from the quantitative approach. Qualitative data collection focuses on in-depth information based on interviews, case studies or observation with the aim of generating hypotheses or building theory (Eisenhardt 1989).

The difference between the two research methods is that the qualitative research method 'provides less explanation of variance in statistical terms than the quantitative research method' as outlined by Kaplan and Duchon (1988, p. 573). In this regard, the qualitative research method can yield rich explanations of the outcome to be further developed during the building theory stage (Eisenhardt 1989).

There are arguments that the positivist paradigm and the interpretivist paradigm cannot be combined to form 'a mixed paradigm' (Creswell & Plano Clark 2007, p. 15). However, Creswell and Plano Clark (2007, p. 173) also claim that an alternative perspective, pragmatism, 'focuses on the research problems and allows multiple methods to address research problems'. It was deemed that this latter approach could allow the researcher to explore the phenomenon of ICT risk management through the qualitative method and then to refine and explain the qualitative results using quantitative research to resolve the research problem. Thus, pragmatism has been adopted in this research. Based on the research methods outlined above, each one relies on research reasoning which is described in three parts below.

3.2.3 Deductive reasoning

Bryman (2008, p. 9) suggests that deductive reasoning is based on 'the commonest view of the nature of the relationships between theory and social research'. Deductive reasoning starts by generating the hypotheses; then these hypotheses are validated to draw conclusions based on the findings (Bryman 2008). In other words, knowledge is based on concrete empirical evidence as accepted truth which is then validated via the hypotheses through the procedures of quantitative research, rather than through observation as in qualitative research (Bryman 2008; Neuman 2000, 2006; Tashakkori & Teddlie 2003).

3.2.4 Inductive reasoning

Inductive reasoning, in contrast, is based on the premise that knowledge originates from observation of 'the empirical world' through qualitative research (Neuman 2006, p. 60), which is then encapsulated in concrete empirical evidence as theory (Bryman 2008). Furthermore, inductive reasoning is the process whereby the researcher infers probable previous circumstances based on theory developed from observing multiple subsequent circumstances in order to gain an understanding of particular circumstances (Tashakkori & Teddlie 2003). Inductive reasoning provides the direction for the researcher to develop

or confirm a theory generated from the abstract regarding 'concepts and theoretical relationships' (Neuman 2006, p. 60).

3.2.5 Abductive reasoning

Tashakkori and Teddlie (2003, p. 481), Josephson (1996, p. 5) argue that abductive reasoning (founded by Charles Sanders Peirce, 1839–1914) is 'a form of inference that goes from data describing something to a hypothesis that best explains or accounts for the data' as part of mixed methods research. Tashakkori and Teddlie (2003, p. 481) add that 'if the simultaneous application of quantitative and qualitative methods leads to inconsistent or divergent findings representing counter-evidence for previous theoretical assumptions, then a second form of hypothetical reasoning comes into play that Peirce has called abduction or abductive inference'. It can then be argued that quantitative and qualitative findings can sometimes go against previous theoretical concepts; this then can lead the researcher to a view that those particular findings have been discovered to be new and still unknown concepts or rules (Tashakkori & Teddlie 2003). Therefore, this logic allows the researcher to believe that qualitative research and quantitative research can be mixed into a single research method due to the flexibility of this approach. The next section outlines the research purpose, which serves to underline the empirical logic of this research.

3.3 Research purpose

This research aims to investigate how structured approaches to ICT risk management are used successfully in practice in Thai businesses. The research aims to explore and explain how business and technical strategies are planned and conducted in Thai business organisations to achieve successful ICT risk management. More specifically, the research focuses on the development of a single management framework for dealing with ICT risk management in Thai business organisations. Moreover, in this regard the COBIT framework itself stipulates that its framework can complement other standards and frameworks (ITGI 2007), although there is as yet no research that proposes how they can fit together in the context of a structured approach to ICT risk management (Tshinu et al. 2008; Siponen & Willison 2009).

The research objectives are:

- To investigate the current profile of ICT risk management in organisational practices in a sample of Thai business organisations, and

- To identify and then model the success elements of ICT risk management in Thai business organisations.

It is imperative that both exploratory and explanatory research methods are conducted in this research to explore the phenomenon of ICT risk management based on the research objectives. Exploratory research is used to conduct an investigation to identify the practices of ICT risk management in Thai business organisations. Explanatory research is used to confirm the success factors affecting the successful application of ICT risk management planning.

3.3.1 Exploratory research

Neuman (2006) argues that exploratory research needs to be the first stage of research to allow the researcher to explore a particular phenomenon or circumstance (such as ICT risk management in organisations) in order to provide sufficient information to design, develop and execute the next research steps. Neuman (2006, p. 34) further suggests that 'exploratory research addresses the "what" question: "What is the social activity really about?" It is difficult to conduct because there are few guidelines to follow'. This implies that, in this research, the purpose of exploratory research is to enable the researcher to understand the circumstances of ICT risk management in organisations in the context of social reality. It also implies that the purpose of this exploratory research should be to identify the real social activity that needs to be explored through framework and standard (e.g. the COBIT framework and the ISO/IEC 17799 standard) that deal with ICT risk management in organisations. However, in this area of study there are few guidelines to help practitioners or researchers; indeed, successful ICT risk management in organisations has been a challenge requiring further attention for over a decade (Coles & Moulton 2003; Segars & Grover 1996; Teneyuca 2001).

3.3.2 Explanatory research

Explanatory research is another research method. As Neuman (2006) suggests, the purpose of explanatory research is to describe the particular phenomenon or circumstance, in this case ICT risk management, in the organisational context. Neuman (2006) also notes that explanatory research is built from exploratory research in order to discover the reasons why something occurs after analysing the qualitative data. Explanatory research is generally focused on 'why' questions in order to provide empirical evidence to either support or deny the exploratory research findings (Neuman 2006; Osborne 2008). Furthermore, it helps the researcher to extend the explanations in

relation to an issue from those identified through previous research or research methods in a single study (Neuman 2006). In the context of ICT risk management, it can also allow the researcher to validate new issues with different types of samples by conducting surveys as part of the quantitative method, in order to strengthen their generalizability as an explanation of 'empirical evidence to support it [the qualitative findings] or against it [the qualitative findings]' (Neuman 2006, p. 35).

In light of the above discussion, the purpose of this research is to undertake exploratory sequential design which will be used to develop a research instrument in order to validate and explain new issues using explanatory research to strengthen their generalizability. In this research, exploratory research was conducted through case studies to allow the researcher to obtain accurate and in-depth information regarding ICT risk management in organisations. In contrast, explanatory research helped the researcher to deal with a large sample size by conducting a survey in order to test the conclusions of the exploratory research. The sequential research design between qualitative and quantitative methods is aimed at the 'triangulation of method' (Neuman 2000, p. 125). The following section outlines the case study design used as the basis of the exploratory research.

3.4 Case study design

Benbasat et al. (1987, p. 369) suggest that 'case research strategy is appropriate for certain types of research problems: those in which research and theory are at their early, formative stages' [Roethlisberger 1977], and 'sticky, practice-based problems where the experiences of the actors are important and the context of action is critical [Bonama 1983]'.

This implies that case study design is appropriate to building theory when the particular phenomenon is at a formative stage. Therefore, a case study helps the researcher to scrutinise the phenomenon in 'its natural setting, employing multiple methods of data collection to gather information from one or a few entities [people, groups or organizations]' (Benbasat et al. 1987, p. 370). The advantage of the case study is that it helps the researcher to obtain in-depth or rich information based on its natural context (Benbasat et al. 1987). Either single or multiple cases can be utilised as part of the case study design (Yin 2003; Benbasat et al. 1987; Darke et al. 1998).

3.4.1 Single case study design

Yin (2003, pp. 39–42) asserts that 'there are several circumstances and five rationales to be represented in a single-case design'. Firstly, the critical factor in testing a well-formulated theory is that the propositions are clearly defined to test as being either true or false in order to confirm, challenge or extend the theory (Yin 2003). Secondly, extreme or unique cases need to be identified as those that occur in very unusual circumstances (Yin 2003). The third rationale is completely different from the second in that it involves a single case study that is used to report an ordinary situation (Yin 2003). Fourthly, the revelatory case entails circumstances when the researcher has an opportunity to observe and analyse a normally inaccessible phenomenon (Yin 2003). Lastly, a longitudinal case involves circumstances when the researcher is allowed to observe two or more different times among which the conditions affecting the phenomenon may change (Yin 2003). Benbasat et al. (1987, p. 373) argue that a single-case study is used 'before theory generation and after theory testing; and it is used to test the boundaries of well-formed theory'.

3.4.2 Multiple case studies design

Multiple case studies design is commonly defined as including more than one occasion of data collection and analysis of a single case study (Yin 2003). This design is normally used to generate and confirm hypotheses (Benbasat et al. 1987) and to build theory (Eisenhardt 1989). Multiple case studies design allows the researcher to cross-analyse the qualitative data among the cases in order to triangulate the qualitative findings (Eisenhardt 1989). Benbasat et al. (1987), Gable (1994) and Yin (2003) also state that multiple case studies design is desirable when the objectives of the research are description, theory building and/or theory testing. Lee (1991) adds that multiple case studies design enables the researcher to formulate verbal propositions on the basis of the qualitative findings for validation during the stage of quantitative research. These verbal propositions then are validated, confirmed or disconfirmed according to the rules of mathematics (Lee 1991). The multiple case study approach was used in this research. This research used techniques to cross-analyse the data from the cases in order to generate a number of propositions or hypotheses to provide a basis, through a survey, for validating, confirming or disconfirming the case study findings.

3.5 Research design

An exploratory research method was adopted in this research. The research was divided into three phases, as represented in Figure 3-1. The first phase of the research involved

a multiple case studies design embedded in exploratory research aimed at assisting the researcher to understand the phenomenon of ICT risk management in organisations. The multiple case studies design phase began with the data collection from semi-structured interviews conducted (Eisenhardt 1989) in six Thai businesses. Content and thematic analyses were used to scrutinise the qualitative data drawn from across the cases in order to come up with reliable and valid qualitative findings (Luborsky 1994; Grinnell 1985).

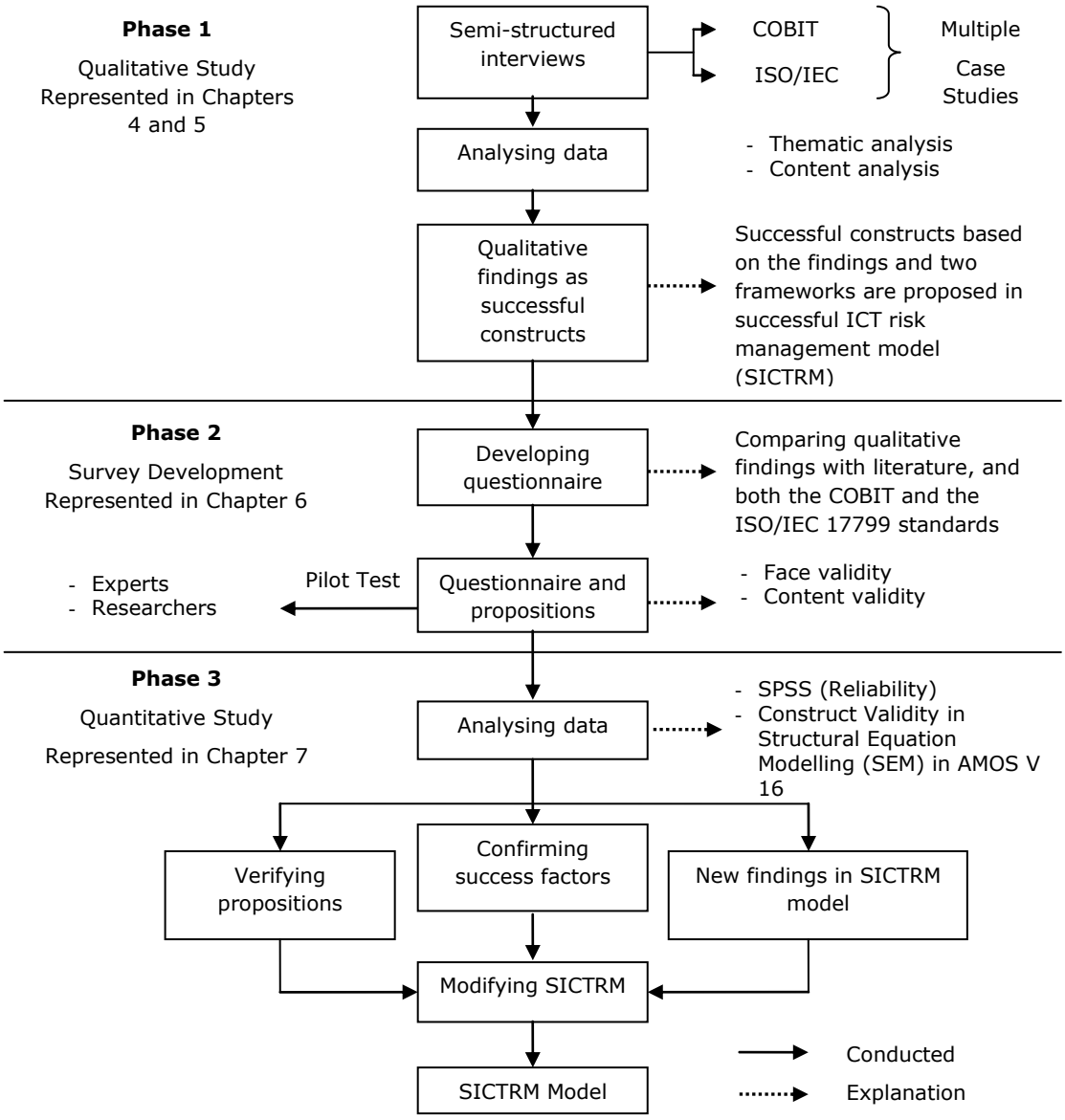


Figure 3-1: Sequential data analysis procedures in embedded exploratory and explanatory designs

Source: Adapted for this research from Creswell & Plano Clark (2007, p. 76)

In the second phase, the issues identified in the case study findings were used to synthesise generalisations and form hypotheses, also using the conclusions drawn from the literature review on ICT risk management. The last step involved using the outcomes of both the survey research and the case studies to validate the propositions, to strengthen definitions of the issues identified, and to establish a successful ICT risk

management (SICTRM) model. The quantitative data were analysed utilising the Social Package for Social Science (SPPS V 16) to validate their reliability. Furthermore, the reliability and validity were scrutinised again using structural equation modelling (SEM) in AMOS V 16 and V 18 in order to validate, confirm or disconfirm propositions, constructs and to propose the new model. Details of each phase in the research design process are outlined below. On the other hand, explanatory research was also used to confirm the variance of circumstance in relation to ICT risk management in an organisation.

3.5.1 The first phase: qualitative study

This phase helps the researcher to 'investigate the current profile of ICT risk management in organisational practices in a sample of Thai business organisations' (refer to the research objective Chapter 3, p. 54). Therefore, this research initially employed the exploratory case study method (Shanks et al. 1993; Yin 1994; Cavaye 1996) as the first stage to explore ICT risk management in organisations.

The case study method was used to investigate the perceptions of senior management regarding ICT risk management processes by focusing on decision-making in this area (Eisenhardt 1989). It also helped the researcher to generate a conceptual framework and hypotheses for later testing (Eisenhardt 1989). Moreover, case study research allowed the researcher to use a combination of data collection methods such as qualitative data (semi-structured interview) and quantitative data (questionnaire) (Eisenhardt 1989). The case study method suits many situations in social science research, such as:

- policy, political science, and public administration research; and
- organisational and management studies (Yin 1994, p. 1).

The main thrust of case study research according to Yin (1994, p. 12) is to examine the following topics: 'decisions, individual, organisation, processes, programs, neighbourhoods, institutions and events'. These topics were applied in this research to understand the decision-making processes of senior management in planning to deal with ICT risk management in their organisation.

Therefore, case study research is useful when a phenomenon is broad and complex, when in-depth investigation of a holistic nature is needed, or when a phenomenon cannot be studied outside the context in which it occurs (Benbasat et al. 1987; Yin 1994). The case study method is more broadly used for exploration and hypothesis generation, but can also be used for providing explanations and for testing hypotheses (Benbasat et al. 1987). This research used multiple case studies to help the researcher generate hypotheses to later confirm using a survey (Benbasat et al. 1987).

Exploratory research was adopted as an approach in this study to explore and seek detailed understanding of the application of existing theory to what is happening in the real world of Thai businesses with respect to ICT risk management (Scapens 1990). Such research is appropriate when there is little knowledge in the area or when there is no available information on similar empirical studies or problems (Cavana et al. 2001).

To explore and understand the phenomenon of ICT risk management in an organisation in the context of exploratory research, multiple case studies were used to draw a holistic picture of the phenomenon (Figure 3-2). The researcher needed to understand the real activity and organisational context of ICT risk management planning in practice (Klein & Myers 1999) in order to synthesise all of the necessary factors impacting the particular phenomenon. Furthermore, the researcher explored not only the 'how' of ICT risk management planning but also the reasons behind such planning.

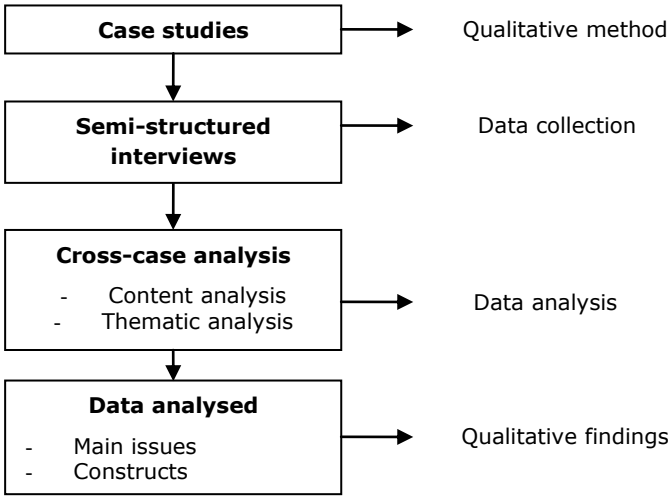


Figure 3-2: Qualitative data analysis

Sampling method and unit of analysis

A purposive sampling method was utilised to select the right participants in each case. Creswell and Plano Clark (2007) argue that the purposive sampling method helps the researcher to intentionally seek and select the required information concerning the primary phenomenon under study, such as ICT risk management planning.

Members of senior management and the operational managers were the appropriate persons for selection in this case, as they make the decisions related to organisational planning (Morris & Pushkin 1995; Groves 2003; Gordon et al. 2006; Myler & Broadbent 2006). Furthermore, senior management comprised the unit of analysis in this research (Benbasat et al. 1987). The senior management level of an organisation is necessarily involved in the major types of organisational planning (such as ICT risk management planning) which are conducted as part of the top-down approach to organisational ICT planning (Stoneburner et al. 2002). On the other hand, the operational manager also

helps an organisation reflect the operational plan to supplement the corporate plan (Gordon et al. 2006; Groves 2003; Myler & Broadbent 2006).

Sample

The sample in this research was purposively selected because the researcher believed that the experience of the participants is imperative, and that in this way the researcher would obtain rich information about ICT risk management in the case study organisations (Neuman 2000; Creswell & Clark 2007). Senior management was selected for the reasons outlined in the previous studies mentioned, as these individuals were able to offer insight into perceptions of the top-down approach in each case because they had the ability to enrich and take charge of ICT risk management in the context of a range of processes regarding ICT governance (Sohal & Fitzpatrick 2002; Schwarz & Hirschheim 2003; Poore 2005; ITGI 2007). Operational staff were also used in the multiple case studies to enrich the information obtained on management perceptions in relation to the bottom-up approach regarding information security governance (Solms 2005a; ISO/IEC 2005).

Site selection

Six case studies embedded in four types of business—banking, telecommunication, software development, and international consulting firms—were conducted to investigate perceptions and experiences of ICT risk management. These cases were selected because the business transactions and operational processes for each of these fields explicitly relate to internal control, information and communication technology (ICT) management and information security (IS) management regarding ICT risk management Moreover, case studies D, E and F elaborated the consulting role in ICT risk management to their client on the way of consultation perspective. For example, the business transactions and processes in these case study organisations are enabled through ICT infrastructure, and all of these businesses control ICT infrastructure through ICT management and IS management. This is important for this research because the COBIT framework, as suggested by the Information Systems Audit and Control Association (ITGI 2006a), provides a framework that enables an organisation to control business and ICT transactions. In contrast, the ISO/IEC 17799 standard, originally published by the International Organisation for Standardisation (ISO) and the International Electro-Technical Commission (IEC) (ISO/IEC 2005), provides a framework for an organisation to control information security, which is more technically oriented.

Data collection

Semi-structured interviews were conducted using open-ended questions during the period of June to September 2007. All interview questions are presented in Appendix A2,

and these interview questions were constructed based on both the COBIT framework and the ISO/IEC 17799 standard regarding key concepts of ICT risk management.

The open-ended questions enabled the researcher to gain an insight into which ICT strategies were deployed through ICT risk management processes in each organisation, what members of senior management thought about the business, and what technical approaches were adopted as part of annual organisational planning; the interviews also sought to determine whether the action plans were seen to be effective in preventing, mitigating and avoiding ICT risks.

The researcher also collected critical information about whether both staff levels were aware of the ICT risks in handling the complexity of ICT systems. The researcher firstly sent an invitation letter, including the researcher's contact details, to the selected sample (e.g. senior management such as President, Vice-President and Manager and operational managers) inviting them to participate in the study (reproduced in Appendix A1). The responses were sent back to the researcher by email. Then the researcher arranged a suitable time with participants to conduct the interview session. Furthermore, email communication between the researcher and the interviewees was maintained for the purposes of validating the findings of the research.

Semi-structured interviews were deemed to be an appropriate method in this study. The use of multiple case studies meant that the researcher in this study was able to gather in-depth information regarding ICT risk management planning in an organisation (Yin 2003; Eisenhardt 1989). Furthermore, the researcher was able to build the theory and generate propositions to be tested in the next stage.

Each interview session lasted approximately one hour. The interview topics included ICT risk management processes and the success of ICT risk management in the participants' organisations using the COBIT framework and ISO/IEC 17799 standard. The interviews were digitally recorded, after the participants' consent was obtained, to ensure accuracy.

The interviews were terminated once the data obtained was seen to be sufficient (Glaser 1967; 1977). In cases where some of the issues regarding the ISO/IEC 17799 standard and the COBIT framework could not properly be translated into Thai, English was used instead. There were no problems regarding English comprehension in the case of senior management staff, as they generally possess higher education backgrounds and are bilingual (in English and Thai). However, when some participants did not understand any particular question the researcher explained the question in Thai.

Ethics and privacy

An invitation letter was sent requesting participants' consent (refer to Appendix A1) prior to the interview process starting. The data collected from the interviews were collated so

that individuals could not be identified. Participants were able to withdraw partially, completely and/or refuse to answer any questions at any time. The privacy and confidentiality of the information provided by subjects, and their anonymity, were strictly maintained. Digital files and transcripts have been securely held in a locked cabinet and a password-protected computer used by the researcher. Strict confidentiality has been and maintained at every stage of the research. All digital copies and transcripts of the interviews are securely stored and must be for at least five years from 2010 when the investigator has completed the doctoral thesis. The identity of participants is disclosed in this research project only when there is the participant's consent. Information is presented in a manner such that no participant's identity can be determined or inferred from the text.

Data analysis

The recorded interviews were transcribed by the investigator in Thai. All transcribed interviews were then carefully translated from Thai into English. During the translation, the researcher repeated the translation several times in order to maintain the accuracy of transcriptions. Transcriptions were then checked by another bilingual researcher to ensure accuracy.

After transcribing from Thai to English, the researcher examined all of the data in order to gain a general understanding of the dataset (Creswell & Plano Clark 2007). Furthermore, the researcher maintained objectivity during content analysis of the reasons elicited from the 'how', 'what', 'why' and 'which' open-ended questions (refer to Appendix A2), in order to ensure the data collected was represented accurately (Krippendorff 2004).

The second part of the qualitative analysis entailed thematic analysis, which helped the researcher to focus on repetitive statements (Braun & Clarke 2006; Luborsky 1994; Weitzman & Levkoff 2000). Luborsky (1994, p. 189) suggests that this analysis involves the 'simple chore of reading through notes and transcripts to identify recurrent statements'. Furthermore, recurrent statements provided the researcher with insight into the perceptions of senior management and operational managers in relation to planning ICT risk management.

After the qualitative data were analysed, the findings of the case studies were used to identify the successful dimensions (the terms 'dimension' and 'construct' are used interchangeably in this research) for the application of both the COBIT framework and the ISO/IEC 17799 standard in ICT risk management in the organisations studied. The qualitative findings led to the development of hypotheses for successful ICT risk management to be validated during stage three. The survey construction for that part of the research is discussed in the next section.

3.5.2 The second phase: survey development

The survey was used to help the researcher to 'identify the success elements of ICT risk management in Thai businesses organisations' (refer to the research objectives in Chapter 3, p. 55). This phase of the research began with mapping the qualitative findings with the COBIT framework and the ISO/IEC 17799 standard by using the following guidelines:

- Aligning COBIT®, ITIL® and ISO/IEC 17799 for Business Benefit: Management Summary (ITGI/OGC 2005);
- Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit: A Management Briefing From ITGI and OGC (ITGI/OGC 2008);
- COBIT MAPPING: Mapping of ISO/IEC 17799:2005 with COBIT® 4.0 (2006) (ITGI 2006);
- COBIT® 4.1 (ITGI 2007); and
- Information technology – security techniques – code of practice for information security management 2nd ed. © (ISO/IEC 2005).

These guidelines were published by the IT Governance Institute (ITGI), the Office of Government Commerce (OGC), the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The guidelines, in conjunction with the related research literature regarding the COBIT framework, the ISO/IEC 17799 standard and ICT risk management, were mapped with the qualitative findings to construct the survey. Based on the theoretical concepts above, the survey was constructed with a clear direction and theoretically driven instrument according to measurement theory (refer to Chapter 6).

The survey construct (outlined in Chapter 6) was based on the qualitative findings mapped with the guidelines and the findings drawn from the relevant literature. The mapping of the findings, guidelines and related literature was then scrutinised to propose the propositions and constructs that formed the conceptual model, derived from the themes identified in stage one, in order to validate, confirm or disconfirm their relationships in stage three.

A seven-point Likert scale was used in this research (Symonds 1924; Miller 1956; Finn 1972; Cox III 1980; Cicchetti et al. 1985; Oaster 1989). This tool allowed participants to indicate their level of agreement with the particular statement or any kind of subjective or objective evaluation of the statement (refer to Appendices B5 and B6). This scale was divided as follows: (1) strongly disagree, (2) moderately disagree, (3) slightly disagree,

(4) neutral, (5) slightly agree, (6) moderately agree, and (7) strongly agree (Harris 2007). After constructing the survey, the questionnaire was sent to the sample, leading to the third stage of the research.

3.5.3 The third phase: quantitative study

This phase was undertaken to help the researcher to 'model the success elements of ICT risk management in Thai businesses organisations' (refer to the research objectives in Chapter 3, p. 55). The survey research investigated the success dimensions that arose from the interview transcripts, which was then used to reconfirm or disconfirm the particular dimensions. The survey asked about success in ICT risk management from the perspective of members of staff from two position levels (the management level and the operational level) within an organisation, by focusing on discussion of both the COBIT framework and the ISO/IEC 17799 standard.

Population

The population for the sample used in this research was comprised of organisations listed on the Stock Exchange of Thailand (SET). The choice of sample was based on an examination of the organisational structure, processes and operational transactions of the organisations relating to business, information and communication technology (ICT), and/or information security (IS) processes. Based on the results of this examination, the researcher was confident that the organisations listed in the sample drawn from the SET use both the COBIT framework and the ISO/IEC 17799 standard, because using of both standards was declared in an annual report of each organisation. The sampling method is further considered below.

Sampling frame

The sampling frame focused on participants who are specifically familiar with ICT risk management planning. Therefore, in this study the sampling frame was stratified from the total population (i.e. all listed organisations in the SET) into a subpopulation based on the (a) banking, (b) technology, and (c) insurance sectors (Neuman 2000). Each sector was identified by the organisational characteristics outlined below.

Position level: several researchers have identified that the position levels which influence the planning of ICT risk management include the management level (Bodnar 2006; Damianides 2005; ITGI/OGC 2005; ITGI 2005, 2006a, 2007; Khan 2006; Lainhart 2000, 2001a, 2001b; Smith & McKeen 2006) and the operational level (Gordon et al. 2006; Groves 2003; Myler & Broadbent 2006). This means that the planning of ICT risk management in organisations involves staff members from these two position levels.

Department: ICT risk management mainly relates to ICT control and audit, which involve the accounting, internal audits, information technology, information security and risk management departments (Leung et al. 2003; IIA 2005; Pickett 2005; Hardy 2006).

In conclusion, three indicators—type of business, position level, and department—were factors in the researcher's choice of sample for the survey. The organisational characteristics are also based on the assumption that these groups of people are representative of practitioners who are familiar with ICT risk management in an organisational context. Therefore, 11 banking, 25 technology and 17 insurance organisations comprised the sample in this research.

Sampling method

Stratified random sampling based on the sampling frame was adopted because ICT risk management in organisations is normally related to a specific function (Tashakkori & Teddlie 2003). Proportional stratified random sampling was identified by type of business, position level and department in each organisation under study (Tashakkori & Teddlie 2003). This technique helped the researcher to avoid sampling errors and to obtain the right representative sample (Neuman 2006). Therefore, this technique limits the number of samples (Neuman 2006). This technique allows the researcher to divide the population into subpopulations (strata) and the sample into each subpopulation (Neuman 2006). The sample is further discussed below.

Subpopulation

The subpopulations in this research were determined by type of business, position level and department based on the selection of companies from the SET website (SET 2008). This included 11 banking organisations, each consisting of five departments, and each department comprising three management and three operational levels (SET 2008). Secondly, there were 25 technology organisations, 18 of which had three departments, while the remaining seven organisations had four departments; each department had three management levels and three operational levels. Lastly, 17 insurance organisations were included, each consisting of three departments, each with three management levels and three operational levels.

The rationale for defining three samples in the management level and three samples in the operational level is that fixed samples would have the same chance of being chosen for the stratified random sampling by the researcher (Neuman 2006). Therefore, a group of management level staff was chosen to represent the position above assistant head of the department in each organisation; and a group of operational level staff representing the operational staff of each department in each organisation was selected.

Table 3-1: The subpopulation stratified from the population

Type of Business	Number of Organisations	Number of Departments	Number of People in Each Position Level		Total
			Management Level	Operational Level	
Banking	11	5	3	3	330
Technology	18	3	3	3	324
	7	4	3	3	168
Insurance	17	3	3	3	306
Total	53				1,128

Sample size

According to stratified random sampling, the population was divided into subpopulations (refer to Table 3-1). Israel (2003, p. 1) and Miaoulis and Michener (1976) suggest that sample size criteria need to determine 'the appropriate sample size: (a) the level of precision, (b) the level of confidence or risk, and (c) the degree of variability in the attributes being measured'. Therefore, the formula suggested by Yamane (1973) was used to calculate the appropriate sample size for this research. This simple formula is as follows:

$$n = \frac{N}{1 + N(e)_2}$$

where n is the appropriate sample size, N is the population size (which this research refers to as subpopulation), and e is the level of precision which is a 95% confidence level and P = .05. Thus, n is equal to

$$295 = \frac{1128}{1 + 1128(0.05)_2}$$

According to the above result, this study requires at least 295 valid respondents in order to allow the research findings to be generalised for a larger population. The number of achieved useable responses received was 302 (refer to further discussion in Chapter 7).

Response rate

Neuman (2006) and Saunders et al. (2003, 2007) recommend that the formula for the response rate be calculated according to the following:

$$\text{total response rate} = \frac{\text{total number of responses}}{\text{total number in sample - ineligible sample}}$$

In the above formula, the total number of responses is the number of questionnaires completed by participants. The total number in the sample is the number of invited participants. The ineligible sample is the number of inexperienced practitioners, defined as those who lack experience of ICT risk management in an organisational context. The resulting total response rate is discussed in Chapter 7.

Pilot test

Prior to launching the survey, the questionnaire was pilot-tested to validate the content and this was generated first as an English version and then in Thai. Content validity and reliability were considered during the pilot-test phase. Two bilingual researchers were used to validate the items representing sense and meaning. Ten experts were then engaged to validate understanding of each question in the questionnaire. It was then suggested that the researcher make a minor change to the expression 'same pattern file' (in the Thai version) in question 50 because the meaning was not clear. This question was revised to 'the data and information was treated using SAP software; may not be treated using other software'. After validating the questionnaire, the surveys were sent out by mail to the stratified subpopulation.

Thai translation

The data collection took place in Thailand. To avoid errors and biases in the data, the researcher needed to ensure content validity of the questionnaire as English (Appendix B5) is not an official language of Thailand. It was imperative that translation of the questionnaire from English to Thai accurate retain the precise sense and meaning of the responses. Thus, translation of the questionnaire was conducted. The invitation letter, the plain language statement (Appendices B1, B2, B3 and B4), the description of the process of distribution and collection, and the survey instructions were also translated (Appendices B5 and B6). Five native Thai speakers familiar with both Thai and English grammar translated and then cross-checked these documents. The complexities of both Thai and English grammar were carefully considered during this stage to ensure consistency of meaning between the Thai and English versions of the questionnaire.

Data collection

The survey construct is presented in Chapter 6, and this research used 'the tailored design method' suggested by Dillman (2007) to collect the data. Dillman (2007, p. 29) claims that the 'Tailored design method is a set of procedures for conducting successful self-administered surveys that produce both high quality information and high response rates'. This set of procedures includes writing the questions, constructing the questionnaire, survey implementation and reducing survey errors (Dillman 2007). This implies that this survey not only improved the quality of the questionnaire but also that the questionnaire could reduce and avoid the sources of survey error which cover:

- sampling error: the result of surveying only some and not all participants;
- coverage error: the result of not allowing all members of the survey population to have an equal or known chance of being sampled for participation in the survey;
- measurement error: the result of poor question wording or questions being presented in such a way that inaccurate or uninterpretable answers are obtained; and
- non-response error: the result of people who respond to a survey being different from sampled individuals who did not respond, in a way that is relevant to the study (Dillman 2007, p. 11).

The mailed survey stage was conducted during the period of May to August 2008. The surveys, with a running number recorded on each questionnaire, were sent to the relevant departments in each organisation.

The survey instruments were randomly distributed among the management level and operational level staff who were willing to participate. Mail was sent to the departments without addressing any specific person or position. This correspondence included: (1) an outline of the required number of samples; (2) the invitation letter; (3) a plain language statement of the research project; (4) an outline of the process of distribution and collection; and (5) the survey instructions (Appendices B1, B2, B3, B4, B5 and B6). The invitation letter was addressed as 'To whom it may concern', so that the sample was randomly selected once the mail was opened. Moreover, this research assumed that the respondents would be sourced from either the management or the operational levels because question number 2 asked for the position level of the respondents (refer to Appendices B5 and B6).

Data analysis

In the second phase, the questionnaire was constructed based on the theoretical concepts of measurement theory. The qualitative findings enabled the dimension to be explored for the conceptual model to then be validated. Exploring the dimensions during the second phase did not necessitate validation of the constructs using exploratory factor analysis (EFA) (Hair et al. 2006; Myers & Oetzel 2003). Myers and Oetzel (2003) conducted their research using qualitative design initially, followed by quantitative design. On the basis of their qualitative findings, they proposed the dimensions represented in their conceptual model, and then validated this with confirmatory factor analysis (CFA) rather than EFA. Hair et al. (2006) also suggest that EFA is not needed when the construct is conceptualised according to the theoretical concepts of measurement theory. Byrne (2001, p. 5) adds that EFA is designed for situations where links between the observed (the measures or items) and latent variables (the constructs)

are unknown or uncertain. In contrast, CFA is appropriate when the researcher has some knowledge of the underlying latent variable structure (Byrne 2001).

Therefore, the analysis of constructs and of the conceptual model was begun with a reliability test of the instrument using SPSS V 16 (see Chapter 7). The reliability and validity tests were used again to validate the constructs and the conceptual model using structural equation modelling (SEM) (see Chapter 7). The reliability test is used to assess the degree of consistency between multiple measurements (items or measures) of a variable (construct and dimension) (Hair et al. 2006). It is also used to test the internal consistency among measures underlying one construct or dimension (Hair et al. 2006). It implies that the individual items or indicators of the scale should not only measure the same construct but also be highly intercorrelated (Hair et al. 2006).

Cronbach's Alpha and coefficient H are reliability tests which were used to validate the consistency of measurements in this research (Hair et al. 2006). Cronbach's Alpha should be greater than 0.7 to be an acceptable reliability coefficient (Nunnally 1967, 1978). The coefficient H should also be greater than 0.7 to be acceptable (Nunnally & Bernstein 1994).

According to Hair et al. (2006, p. 137), the validity test must ensure that 'a scale (a) conforms to its conceptual definition, (b) is unidimensional, and (c) meets the necessary levels of reliability, [and] the research must make one final assessment: scale validity'. The validity test is used to represent the degree of accuracy between a set of measures and the concept being studied (Hair et al. 2006).

In terms of SEM, this research utilised CFA to conduct the validity test (Hair et al. 2006).

> *'CFA is a special type of factor analysis and is the first part of a complete test of a structural model. Unlike EFA, the researcher must be able to tell the SEM program which variables belong with which factors before an analysis can be conducted. The CFA not only must provide acceptable fit but also must show evidence of construct validity. When a CFA model fits and displays construct validity, the measurement theory is supported'.* (Hair et al. 2006 p. 779)

According to Hair et al. (2006), CFA is the greatest advantage to be gained from SEM because it allows the researcher to assess both the validity test and measurement theory. Construct validity occurs when the measure is a good representation of the variable that the researcher intends to measure (Holmes-Smith 2007). To establish construct validity, convergent, discriminant (Campbell & Fiske 1959; Hair et al. 2006) and nomological validations are required (Hair et al. 2006).

Convergent validation is used to assess the degree to which two or more items of the same concept or construct are correlated (Hair et al. 2006). In other words, a high degree of correlation among measures, items or indicators reveals that 'the scale is measuring its intended concept' (Hair et al. 2006, p. 137). This is a measure of the scale of the direct structural relationship between an observed variable (item) and a latent variable (construct). Convergent validity is met when standardised loading estimates are greater than 0.7 and correspond approximately to the score of reliability of items being greater than 0.50 (Hair et al. 2006).

Discriminant validity is used to assess the degree to which two conceptually similar concepts are distinct (Hair et al. 2006), and thus reflects the extent to which the constructs in a model are different. This implies that two constructs should be interrelated but any significant correlations between them should be less than 0.90 or 0.85 (Hair et al. 2006; Kline 1998, 2005).

Lastly, Hair et al. (2006, p. 778) argue that 'the processes for testing face validity and nomological validity are the same whether using CFA or EFA'. Nomological validity is checked to ensure that the correlation among the constructs in a measurement theory makes sense (Hair et al. 2006). Hair et al. (2006) also suggest that face validity must be ensured before any theoretical testing is conducted when using CFA (refer to Chapter 7 for further detail).

Once the reliability and validity of the items, the instrument, the constructs and the conceptual model are ensured, the goodness of fit (GOF) measures can be considered. The GOF is normally used to assess the degree of fit between the construct, the measurement model and the structural model (Hair et al. 2006). This research used two types of GOF: absolute fit and incremental fit indices.

Firstly, the absolute fit index is a group of direct measures that 'show how well the model specified by the researcher reproduces the observed data' (Hair et al. 2006, p. 746; Hooper et al. 2008). This group of indices primarily allows the assessment of how well a researcher's theory fits the sample data (Hair et al. 2006). In other words, the covariance matrix of the specified model is statistically insignificantly different from the covariance matrix of sample data. Therefore, absolute fit indices were used to assess how well the theory of the researcher fit the sample data.

Secondly, the incremental fit index is a group of measures that show 'how well a specified model fits relative to some alternative baseline model' (Hair et al. 2006, p. 749; Hooper et al. 2008). This means that these measures help the researcher to assess the specified model (the model based on the researcher's theory) when compared with the null model (the model based on the observed uncorrelated variables) (Hair et al. 2006).

Therefore, incremental fit indices were used to assess whether the specified model of the researcher was better than the baseline model.

3.6 Conclusion

This chapter has provided the rationale for the choice of the qualitative and quantitative research methods selected to collect and analyse data in this research. The chapter has highlighted the existing research philosophies and introduced the position of this research as pragmatism, on which the approaches to the research questions and the research purposes were based. The researcher utilises a qualitative approach in the first phase to explore the phenomenon of ICT risk management in organisations. The second phase aims to conceptualise the constructs or dimensions that reflect successful ICT risk management in Thai organisations. The researcher then develops a number of hypotheses for validation using a survey and statistical analysis. The third stage adopts a quantitative approach to reconfirm and validate the key factors of ICT risk management in Thai organisations and then to identify the success factors of ICT risk management. The outcomes of Phase 1 of the research are described in the next chapter.

Chapter 4

CASE STUDIES IN THAI BUSINESS ADOPTION OF ICT RISK STANDARDS: CASES A-C

This chapter reports on three case studies of ICT risk management in Thai organisations. Data was collected through semi-structured interviews. The chapter begins with an outline of all six case studies, yet only reports on and discusses the results of case studies A, B and C. The findings of case studies D, E and F are discussed in Chapter 5. Case studies A, B and C explore ICT risk management based on the organisational perspective. In contrast, case studies D, E and F illuminate the practice in terms of both organisational and consulting perspectives.

4.1 Data classification

Initially an analysis of ICT risk management in each organisation was conducted. After examining the data, a thematic analysis of organisational elements related to ICT risk management was undertaken.

There were two types of qualitative data in this research. Firstly, three cases (A, B and C) were investigated in relation to what had been done in the area of ICT risk management in their organisations. Another three cases (D, E and F) were examined in terms of what they had done in their own organisations and with consultation in their clients' organisations about ICT risk management (this process was explained in Chapter 3, p. 61). Therefore, the researcher needed to determine the scope of these case studies and to identify the main actors in each from which participants were selected, the details of which are outlined in Table 4-1.

Table 4-1: Case studies details

Case Study	Type of Business	Number of Employees	Participant Number	Participant Position
A	Tele-communications	5,154	2	- Assistant Vice-President (ICT Audit) - Operations Manager
B	Banking	570	3	- Assistant Vice-President - Division Director (ICT) - Division Director (Internal Audit)
C	Software Development	520	3	- Technical Director - Software Development Manager - Information Security (IS) Manager
D	International Consulting	1,700	2	- Chief Information Officer and Chief Finance Officer (CIO/CFO) - Executive Director (ICT Advisory)
E	International Consulting	700	1	- Executive Director (Risk Advisory)and Chief Information Officer (RAD/CIO)
F	International Consulting	700	1	- Senior Consultant

The next section discusses ICT risk management practice in the case studies.

4.2 Case study A

4.2.1 Organisational profile

This organisation is a well-known telecommunications organisation in Thailand listed on the Stock Exchange of Thailand (SET). This organisation is responsible for several types of business segments related to wireless communications such as network engineering; network planning; equipment procurement and installation; network maintenance; and service commercialisation. Information and communication technologies (ICTs) are widely used for management and organisational processes throughout this organisation and its subsidiaries.

4.2.2 Organisational structure

Roles and responsibilities

This organisation has three structured committees related to ICT risk management (an audit committee, a risk management committee and an enterprise-wide security committee). These committees are among them responsible for ensuring the control of internal management and audit; the protection of business ICT and ICT security processes; and the prevention of risks relating to business ICT or ICT security (Figure 4-1). The Assistant Vice-President explained that:

> *"My organisation assigns the management level to be responsible for different operational areas such as business (e.g. business risks) and ICT (e.g. ICT risks including general ICT and ICT security)."*

The audit committee is responsible for all ICT and non-ICT processes regarding audit planning and methodology. The risk management committee is accountable for all types of risk within all of the eight units and/or departments in the organisation, such as ICT risks, HR risks or engineering risks. The enterprise-wide security committee focuses on handling all types of ICT security risks across all departments in the organisation.

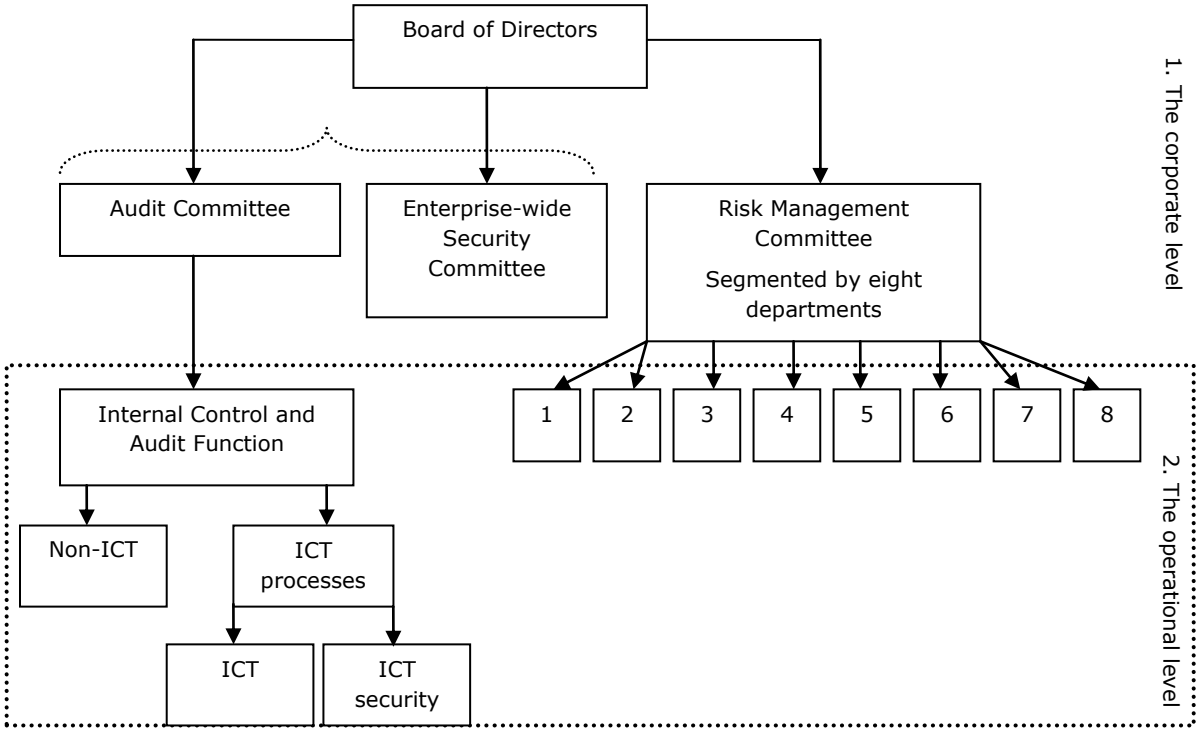


Figure 4-1: Roles and responsibilities: Case study A

ICT risk management is based within two levels of this organisation: the corporate level and the operational level. Furthermore, ICT risk management is treated by the internal audit department as its main responsibility. The internal audit department divides its responsibilities into two areas: non-ICT and ICT processes. Non-ICT processes relate to audit function of documentation, in contrast, ICT processes relate to audit function of computerised systems.

ICT risk management treatment

This organisation conducts ICT risk management at two levels. Firstly, senior management focuses on the corporate level which provides overall information based on the application of the COBIT framework. Secondly, the operations level focuses on specific information related to dealing with ICT risk using the ISO/IEC 17799 standard as a guideline. Once the auditors determine the area of control and audit, they then follow the ICT audit plan. For example, the audit plan in this organisation is based on the audit plan of the Information Systems Audit and Control Association (ISACA), which specifies the directions related to the control and audit of data in operating systems such as Oracle, UNIX or SAP. However, the ISO/IEC 17799 standard is used by all units and

departments in this organisation as a baseline for planning prior to the audit and control phases. An ICT, or business audit, is delivered by senior management to operational staff as part of a top-down approach to ensure that all staff perform consistently. As the Assistant Vice-President described:

> *"My organisation mainly focuses on the top-down approach to control business processes and ICT processes."*

While the Operations Manager explained:

> *"I think the top-down approach is important but it may not cover the operational matters such as ICT security. I think ICT risk management is monitored at both the management and the operational levels."*

Components of ICT risk management

Focusing on only ICT processes, there are two main roles for internal control and audit regarding ICT risk management in this organisation: both general ICT and ICT security are controlled by the internal audit department (Figure 4-2). As the Assistant Vice-President stated:

> *"I think … in order to deal with ICT risk management, we classify ICT into two directions: general ICT and ICT security that can help me to deal with risk appropriately."*

The Operations Manager supported this:

> *"I think to deal with ICT risk management, general ICT and ICT security are focused on."*

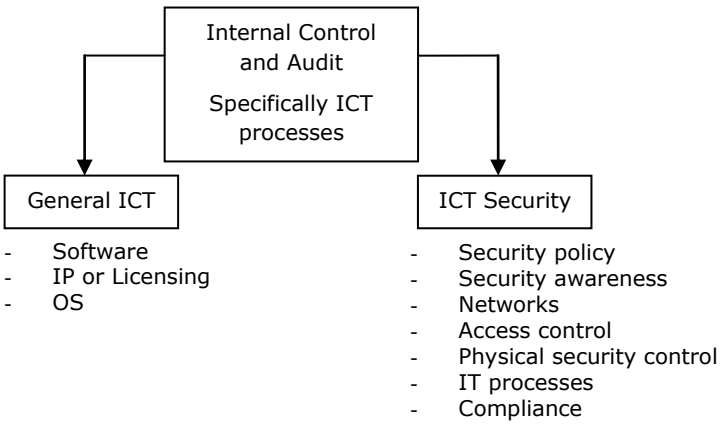


Figure 4-2: Components of ICT risk management: Case study A

The general ICT function includes responsibility for all applications and relates to software, intellectual property and operating systems, as well as related risk management. The ICT security function is accountable for security activity and technical matters related to security. The ICT security function mainly focuses on ICT security, such as ICT security policy, security awareness, networks, access control, physical security control, compliance and ICT processes.

4.2.3 Organisational process

ICT risk management instrument

Interviewees from this organisation believe that the effective management of general ICT and ICT security functions is imperative in order to identify, assess, respond to and monitor ICT risks. This is illustrated in Figure 4-3 below. When applying ICT risk management policy, the organisation must determine the person or persons who must assume responsibility for managing ICT risks. ICT risks will then be identified and assessed according to the degree of impact and probability of occurring as high, medium or low. ICT risks identified and assessed will then be reported directly to a respondent so that he or she can take action to mitigate and closely monitor such risks. After managing the risk, the respondent will present an ICT risk management report to the audit committee to demonstrate how they have dealt with those risks and whether or not they can mitigate the degree of impact and ensure the risk will be maintained at an acceptable level. Subsequently, the audit committee will provide feedback to the respondent. In this regard, the Assistant Vice-President stated:

> *"We have the instrument to deal with ICT risk management; we follow the guideline from the ICT risk management standard. However, we adapt it instead of follow it exactly."*

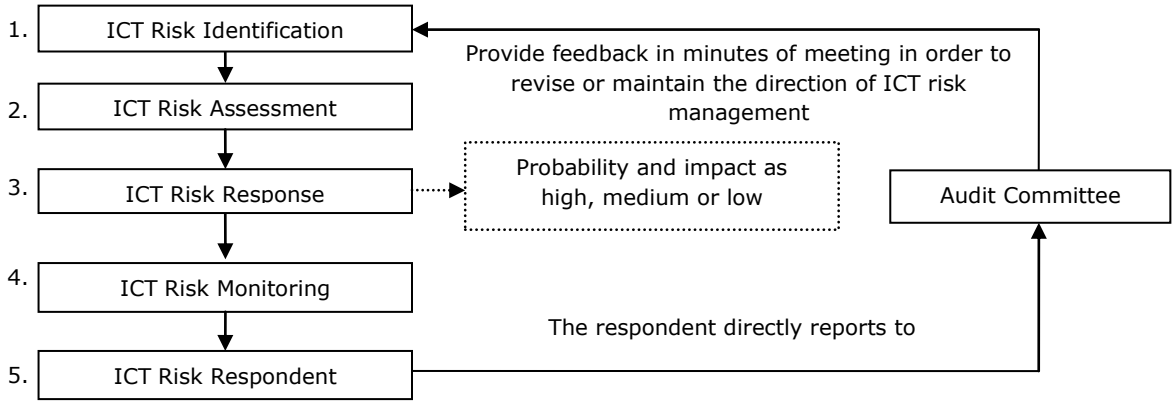


Figure 4-3: ICT risk management instrument: Case study A

ICT risk management plan

This organisation follows the enterprise risk management (ERM)[1] framework as the main control process when dealing with ICT risk management. ERM represents corporate governance regarding business risk management which helps the organisation prevent, avoid and mitigate business and ICT risks. The Assistant Vice-President noted that:

> *"We use the ERM framework as a main process, and then use other frameworks and standards to deal with different directions. For example, if we are looking at ICT risk, we use ICT governance to help us plan ICT process and information security management (ISM) to deal with risks occurring from ICT and information security."*

The Operations Manager added:

> *"In my opinion, I think ICT governance and ISM will help my organisation to deal with ICT risk."*

In terms of the ICT perspective alone, ICT governance in this organisation is based on a main set of guidelines for dealing with ICT risk management. In practice, this organisation has ICT control and audit processes outlined in the corporate plan. The interviewees from organisation A explained that the corporate level plan is divided into three parts: engineering, business and ICT. They also mentioned two specific aspects of management within each of these areas: ICT control and audit; and business control and audit. Specifically, ICT risk management in the corporate plan (i.e. the corporate plan) is focused on ICT risk identification and assessment in order to determine which ICT processes contain a high probability of risk, as well as on an assessment of the degree of impact of this risk. The balanced score card (BSC[2]) technique is used to measure the critical process or processes among all internal processes. The BSC is measured by using a key performance indicator (KPI) to evaluate which critical process is perceived as a

[1] ERM is a process affected by an entity's Board of Directors, management and other personnel, applied in a strategy setting and across the enterprise, designed to identify potential events that may affect the entity, to manage risk to be within its risk appetite, and to provide reasonable assurance regarding the achievement of entity objectives (COSO 2004, p. 2). However, ERM focuses only on business process instead of information technology and/or information security processes.

[2] BSC is a management system that can create breakthrough improvements in such critical areas as product, process, customer, and market development (Kaplan & Norton 1993, p. 134). The scorecard allows managers to 'link long-term strategic objectives with short-term actions' relying on four new management processes (Kaplan & Norton 2007, p. 3). These four new management processes include:

- Translating the vision: helping managers to build a consensus around the organisational vision and strategy.
- Communicating and linking: helping managers to communicate their strategy up and down the organisation and to link it to departmental and individual objectives.
- Business planning: enabling an organisation to integrate business and financial plans.
- Feedback and learning: giving an organisation the capacity of existing feedback and review process called strategic learning. (Kaplan & Norton 2007, p. 3)

Van Grembergen (2000) suggests that business process and IT process are different thereby the measurement and follow-up. Therefore, the business balanced scorecard is needed to adjust IT processes, and these are called IT balanced scorecards for assuring ICT governance.

weakness in terms of being an obstacle to achieving successful business objectives. The BSC measure is clearly defined according to three types of core business objectives—engineering, business and ICT—and concentrates on human resources, business process, technology and systems. The BSC is also defined within the organisation's mission, to meet the targets of the organisation relating to mitigation of ICT risks. ICT processes are monitored as a whole and are associated with organisational internal control and audit.

ICT risk management processes in this organisation include risk identification, risk response and risk monitoring. In particular, all types of risk in this organisation are explained in terms of the probability of each type of risk occurring, and its likely impact, in all departments. The risks are rated as high, medium or low in terms of probability and impact by departments and/or units. The process entails a training program, education program and risk statement that facilitates further action.

Each ICT risk management process is framed in the corporate plan by senior management. Each department must then generate a detailed operational plan, to complement senior management's plan, which fits with the primary goals of the organisation. This process is illustrated in Figure 4-4.

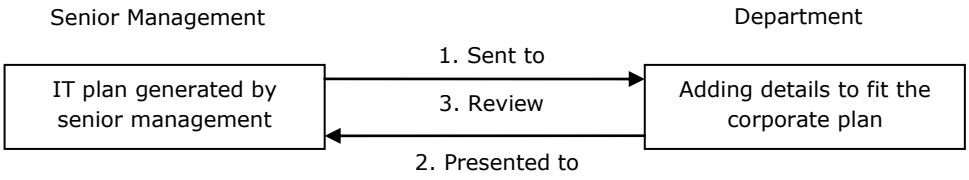


Figure 4-4: ICT risk management plan: Case study A

The details of the main ICT risk management plan of each department are then presented to management for review and further recommendations regarding revision or implementation are offered as needed.

4.2.4 Organisational control

Human resources

Awareness of ICT security is used in this organisation to make risk issues apparent to staff. This program communicates ICT security policy and regulations to all staff, and consists of a delineation of how to manage ICT processes in a secure way, what to do and what not to do, and the penalties for breach of the policy and regulations. All staff are trained in how to use computers appropriately. For example, no staff are allowed to share files, folders or even data with any other staff. E-learning is also provided to educate staff about ICT security awareness. To ensure that employees understand these

regulations, an examination is conducted by the internal audit department. The Assistant Vice-President explained:

> *"Employees are very important to be controlled because they are the key persons who may make risks occur intentionally and unintentionally."*

Control process

To manage ICT security properly, the enterprise-wide security committee has established an ICT security framework for the entire organisation. The framework has also been established in the organisation's subsidiary companies to ensure that their staff are also compliant. Currently, ICT risk management consists of two main approaches to guarantee the quality of ICT control and audit processes (Figure 4-5). Firstly, the organisation focuses on quality assurance to appropriately support staff who handle ICT risk. This means that senior management fully supports staff to manage ICT security closely by incorporating an ICT control and audit mission within the overall business plan. Secondly, an audit-based approach is used to maintain suitable standards of ICT risk management in the organisation. For example, when an ICT risk appears, senior management consults with the respondent or the department over the best means to deal with the risks. The internal audit department takes direct responsibility for following and revising the audit plan, program and/or methodology in responding to the presence of risk.

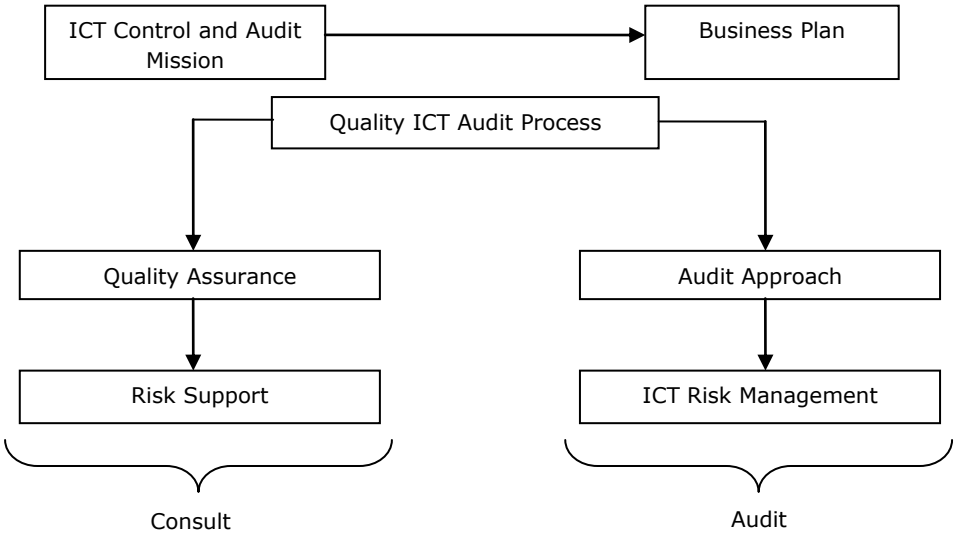


Figure 4-5: Control process of ICT risk management: Case study A

The Assistant Vice-President stated that:

> *"Internal control and audit processes are vital for dealing with risk management."*

The Operations Manager asserted that:

> *"ICT risk management is controlled by focusing on ICT management and ICT security."*

Technology and systems

Thus, ICT risk management in this organisation relates to ICT control and audit. ICT control and audit are focused primarily on two areas: ICT applications, and ICT security given the current circumstances of the organisation. ICT control and audit are concerned with areas such as applications and software; licensing; intellectual property; and software maintenance. ICT security control and audit are major concerns for the organisation, as evidenced by management's recent decision that the enterprise-wide security committee should also monitor these areas. ICT security control and audit cover extensive management of the following: databases, servers, operating systems, networking, other setting configurations, and even penetration tests. To ensure ICT security, this organisation also uses a security scanning tool to inspect and identify any weakness in networks, web servers and other ports, in order to remove any fragile elements.

The Operations Manager revealed that:

> *"My organisation has tools to prevent ICT risk such as the penetration test and security scanning in order to check ICT abuses and ICT disruption."*

4.2.5 Organisational ICT strategy

The organisational ICT strategy in this organisation is based on a top-down rather than a bottom-up approach to ICT risk management (Figure 4-6). As a top-down approach in this organisation, ICT risk policy is directed and controlled by senior management or the Board of Directors. In addition, ICT strategy based on ICT risk policy is delivered to operational staff to follow and implement. While the organisation strongly believes that a top-down approach is best suited to its needs, a bottom-up approach is also used to review the business and operational (i.e. the action plan) plans through the provision of a report from operational staff to the Board of Directors, especially in the security operations area.

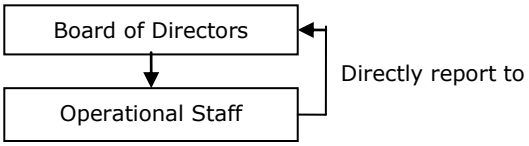


Figure 4-6: Organisational ICT strategy: Case study A

The corporate (or annual) plan or business plan related to ICT is generated every year in order to guide the business direction of the organisation, specifically the direction of ICT. The corporate plan describes the scope or overview of the ICT plan for each year. The ICT plan is developed in detail to cover general ICT management; the ICT security plan; ICT control and audit; and ICT security control and audit. This will then be matched with the action plans of each department (e.g. the internal audit, ICT, accounting or information security departments).

Practically, the operational (or action) plan in this company is derived from using the COBIT framework as the main scope of ICT management and the ISO/IEC 17799 standard as the technical guideline for dealing with ICT risk management through internal control and audit in the organisation (Figure 4-7). Firstly, the COBIT framework is used as the basis for the control objectives to match with both ICT control and audit objectives and business objectives. The control objectives of each domain drawn from the COBIT framework cannot be used immediately as ICT control processes because the control processes need to be adapted to fit with organisational ICT processes.

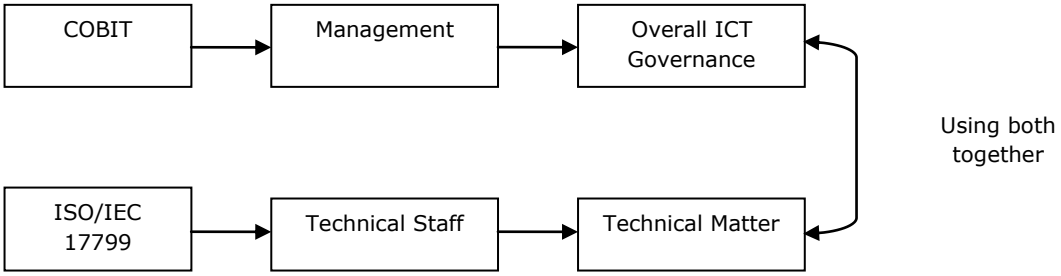


Figure 4-7: Organisational ICT processes: Case study A

Application of the ISO/IEC 17799 standard in this organisation is used to set the technical control of specific technical details in line with the control objectives adopted from the COBIT framework. In contrast, using the COBIT framework or the ISO/IEC 17799 standard alone, according to the respondents, cannot cover the overall control and audit plan they want in place. They argue that the COBIT framework is primarily appropriate for management to generate extensive framework for ICT governance related to ICT risk management. The ISO/IEC 17799 standard, on the other hand, is used to set the focus on the details of technical matters. Although the COBIT framework and the ISO/IEC 17799 standard differ in this way, they can complement each other within the overall ICT risk management plan in this organisation.

4.2.6 Summary

In this organisation, the key factors addressed by, and which were the focus of, ICT risk management were:

- policy;
- management of ICT resources;
- human resource management and planning or the management of people and their behaviour in the organisation;
- information security (IS) management; and
- ICT risk management plan.

Policy for ICT risk management in this organisation is considered to be the key factor driving the business direction. This organisation divides its policy into business, ICT and IS policies for dealing with business and ICT risks. In relation to ICT risks, the interviewees particularly emphasised that ICT and IS policies can help achieve the prevention and avoidance of ICT risk, and the mitigation of ICT risk at an acceptable level.

The management of ICT resources is another concern in this organisation. This key factor primarily involves the management of software applications, networking connections (i.e. internet protocol, or IP), software licensing and operations systems under the umbrella of general ICT control.

Human resource management and planning is also a concern for this organisation. The main foci of this key factor are on raising awareness of human resources, delivering training programs and on staff roles and responsibilities along with ICT risk management planning. This area is also concerned with the strict control of compliance with rules and regulations in the organisation. All staff are required follow organisational policy, rules and regulations.

Information security (IS) management is considered to be the key factor for dealing with ICT risk management planning in this organisation. IS management focuses on the security of ICT systems, through the use of tools such as the penetration test and the security scanning tool. This organisation pays attention to raising security awareness, networking security, access control, physical security control and security in ICT processes in order to achieve the aims of the information security policy.

Lastly, linking this organisation’s practice to the research purposes, this organisation drives ICT risk management planning at two levels: the corporate level and the

operational level plan. However, the main concern of the ICT risk management plan is to implement change through a top-down approach. In other words, the senior management has set organisational policy, management of ICT resources, IS management and human resource management at the corporate level, which indirectly affects the operational planning which is delivered via a bottom-up approach.

4.3 Case study B

4.3.1 Organisational profile

This organisation is a banking institution listed on the SET. This organisation divides its two business segments (the financial segment and internal operations segment) into eight categories: housing loan group; lending group; treasury group; commercial banking group; human resources and administration group; system and technology group; risk management group; and bank operations group. This organisation has invested in ICTs to help facilitating both stockholders and stakeholders. ICT processes are monitored and reviewed by both the internal audit section and the systems and technology section as part of the internal operations segment.

4.3.2 Organisational structure

Roles and responsibilities

The responsibility for ICT risk management lies with the audit committee in this organisation. The audit committee is responsible for both types of business process—non-ICT processes (business risks) and ICT processes (ICT risks)—which relate to the purpose of the general and the ICT audits (Figure 4-8). The audit committee formulates internal control and audit objectives which control data reliability; effective and efficient performance; and compliance and regulatory. This implies that the audit committee is responsible for the control of both non-ICT and ICT processes. The functions of control and audit have their own separate plans.

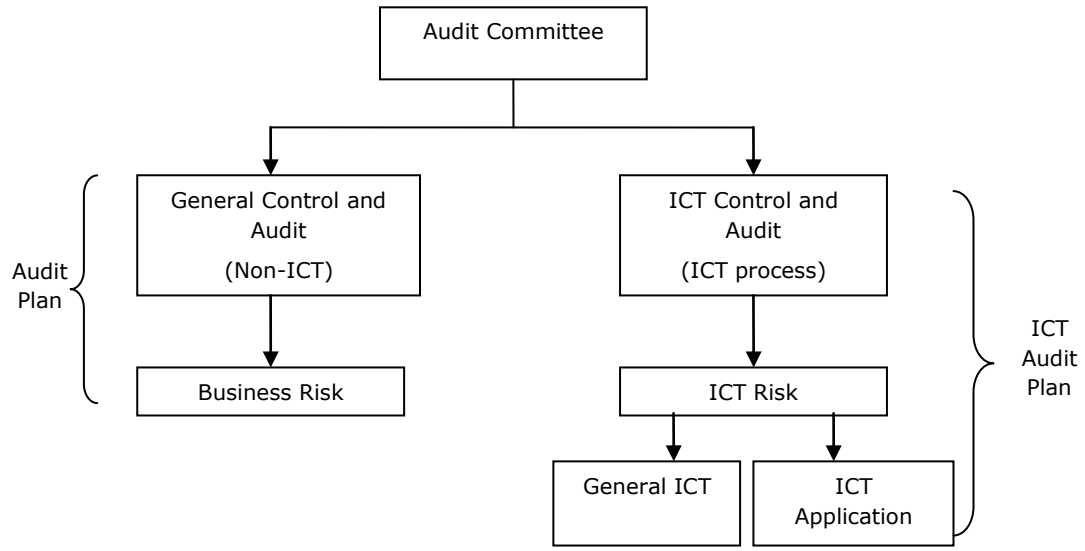


Figure 4-8: Roles and responsibilities: Case study B

The Assistant Vice-President said:

> *"My organisation at the moment has only audit committee to deal with both business and ICT risks which I think it is not enough. However, in the next few years, I think there will be several committees to be responsible for all types of risk."*

The Division Director (internal audit) confirmed that:

> *"The audit committee is responsible for both non-ICT and ICT processes."*

ICT risk management treatment

ICT risk management in this organisation is conducted primarily as a bottom-up process rather than a top-down process in so far as operational management specifies the technical details of general ICT (i.e. ICT infrastructure and ICT risk management) and ICT applications (i.e. software regarding applications, operating systems and networking systems) more clearly than could senior management (Figure 4-9). Operational managers specify the details of technical processes and report to senior management to discuss proposed plans for review and/or implementation by operational staff. In this regard, the Assistant Vice-President explained:

> *"We are in the initial stage of ICT risk management plan; we then focus mainly on the business process first and the ICT process in the next step. We think that the operational level plan approved by the management level can help my organisation deal with ICT risk."*

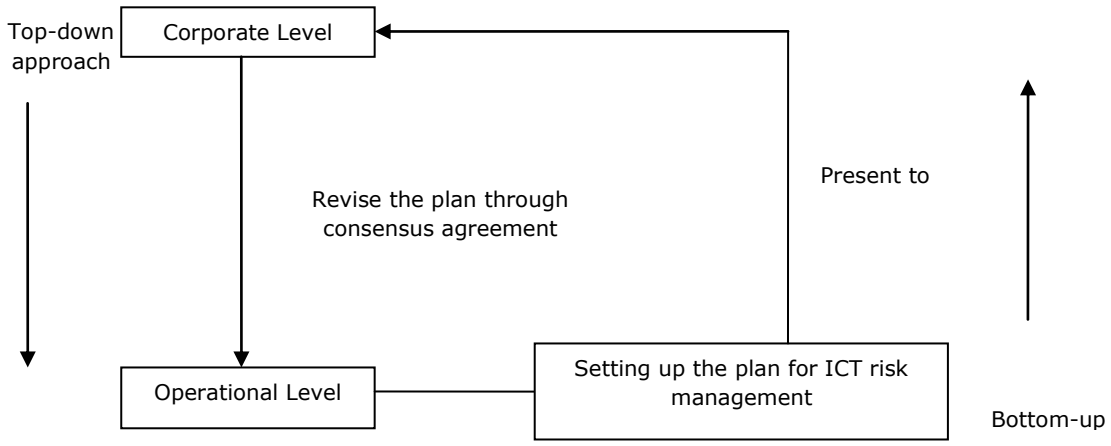


Figure 4-9: ICT risk management treatment: Case study B

Nevertheless, a top-down process is also considered important by senior management in this organisation B. A top-down process is used to revise ICT risk management plans and to translate the corporate plan from the corporate level to the operational level. Therefore, the ICT risk management plan is considered at both the corporate level and the operational level, such that both plans must initially be separated, with a consensus agreement required between both levels on the final organisational plan. Therefore, the top-down approach entails direction from senior management to the operational level regarding its perspective on ICT risk management based on the revision of the operational plan. This approach, the interviewees noted, can also help senior management understand ICT security, ICT security endorsement (i.e. senior management buy-ins) and ICT security advice offered to the Board of Directors (BOD).

Components of ICT risk management

In terms of ICT control and audit, general control (the management of ICT infrastructure and processes) and application control (the management of information security) are the foci in this organisation (Figure 4-10).

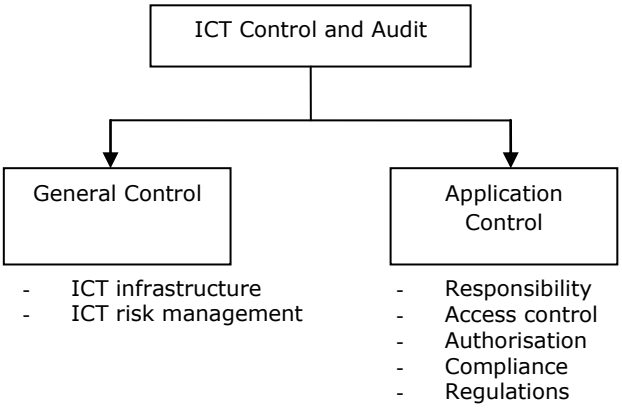


Figure 4-10: Components of ICT risk management: Case study B

This organisation is concerned with the control of networks, configuration and virus patterns as aspects of general control. Another element of general control is ICT risk

management which relies on computer systems management (e.g. ICT management) to manage the risks and ensures the organisation runs effectively through the provision of hardware, software, people-ware and back-up plans.

The second aspect of ICT control and audit is application control, which focuses on roles and responsibilities; access control; data authorisation; compliance; and regulations. In relation to this, the Division Director (ICT) said:

> *"…. my organisation elaborates the control of general ICT and ICT application."*

The Division Director (internal audit) added:

> *"General ICT is about ICT management and ICT application is about all types of software used in the organisation."*

4.3.3 Organisational process

ICT risk management instrument

The ICT risk management instrument used in this organisation consists of five main processes: defining objectives, risk identification, risk assessment, risk control and risk monitoring. The formulation of the objectives of ICT risk management occurs at the corporate level which provides a clear statement for the whole organisation. The organisation further identifies any weaknesses among the business and ICT processes. The weak points in the ICT process among general ICT and ICT applications are identified to be dealt with by individual departments in the organisation. The organisation utilises the COBIT framework to fix weak ICT processes. For example, if the ICT planning process is found to be a weak area, the planning and organising domain within the COBIT framework is used to select the appropriate control objectives to suit the problem in that particular area. As the Division Director (Internal Audit) explained:

> *"I personally apply the ERM framework based on my experience to deal with ICT risk management. The ERM framework helps me to define what the objectives, risk identification, risk assessment, risk control and risk monitoring are considered for dealing with ICT risks, although it mainly focuses on business context but I adopt it for ICT context."*

ICT risk management process

The framework created by the Committee of Sponsoring Organisations of the Treadway Commission (COSO) is used by this organisation to plan its corporate governance in

order to control the business processes as non-ICT processes at the corporate level (Figure 4-11).

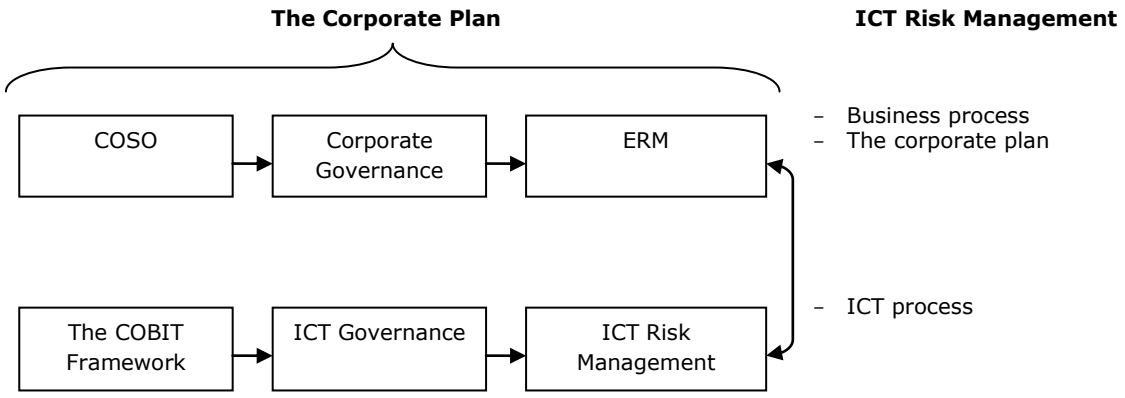


Figure 4-11: The corporate level of non-ICT processes and ICT processes: Case study B

ERM is a mechanism for corporate governance used in this organisation to deal with business risk management. In contrast, the COBIT framework has been adopted for ICT governance to deal with ICT risk management in this organisation. The COBIT framework guides the organisation to define the main scope of ICT control and audit at both the corporate and the operational levels to review ICT systems, applications, operating systems, and networks. However, both of these standards were used to supplement the corporate and the operational plan. The Division Director (Internal Audit) mentioned:

> *"Based on the audit committee, we use the ERM as the baseline to deal with risks; however, we also use the COBIT framework to supplement ICT processes in the business control plan."*

4.3.4 Organisational control

Human resources

According to senior management, employees in this organisation must understand the ICT risk management process, acknowledge that there are ICT risks in their functions and departments, make decisions on whether it is necessary to mitigate ICT risks, and report the occurrence of ICT risk to all relevant departments, as it is not only one department, they argue, that can prevent and mitigate ICT risks.

Senior management in this organisation believe that education and training are also essential, not only for operational staff, but also for management, because all employees must understand their roles and responsibilities as defined by human resources authorisation in order to effectively deal with ICT risk management. The Assistant Vice-President, supported by both Division Directors, agreed with this view:

> *"Our staff are performing well otherwise the risk may occur. Therefore, we provide training for and educating them about ICT awareness and ICT security; although we are just starting to plan information security management."*

Control process

Senior management in this organisation believe that they must ensure that all ICT processes are undertaken properly in each department. There are three main steps involved in the review of ICT risk management processes in this organisation: (a) self-compliance, (b) risk reporting, and (c) risk monitoring from both internal and external auditors (for example, the Bank of Thailand (BOT), the Securities and Exchange Commission of Thailand (SEC), and the Certified Public Accountants of Thailand (CPAs)).

In the view of senior management in this company, ICT risk management relates to ICT control and audit. They argue that effective ICT control and audit regarding risk management needs to include: (a) a general audit manual, (b) an audit program, and (c) a detailed audit methodology.

Audit methodology in relation to ICT risk management is generated from both the COSO-ERM framework and the COBIT framework. Audit methodology is also known by other names, such as audit guidelines, audit program or internal control questionnaire (ICQ). In practice, the COBIT framework is used in this organisation as the main framework to define ICT control objectives and the processes that require attention each year.

The Division Director (Internal Audit) mentioned:

> *"The way to deal with ICT risk, I think we have a clear auditable area to deal with one particular thing. For example, we are focusing on ICT risk; so we provide the plan for ICT area including ICT management and ICT security to control and audit ICT risk properly."*

The COBIT framework is applied in this organisation to guide the overall ICT control and audit but it does not provide much detail on technical terms (Figure 4-12). In this regard, the Division Director (Internal Audit) asserted that another standard or framework is used to handle these technical matters; this might include, for example, some frameworks or standards such as Microsoft Pattern, AS400 and the ISO/IEC 17799 standard. These frameworks are used to solve technical issues depending upon the nature of the auditable area. At the strategic level of planning, it is more important to have detailed guidelines related to information security management. Senior management believes that the ISO/IEC 17799 standard as an exemplar can be used to manage information security (IS). In contrast, the COBIT framework is used in this organisation to cover the scope of internal control and audit to ensure good ICT

governance. Therefore, both the COBIT framework and the ISO/IEC 17799 standard, the respondents claimed, can supplement each other in guiding the ICT risk management planning in this organisation.

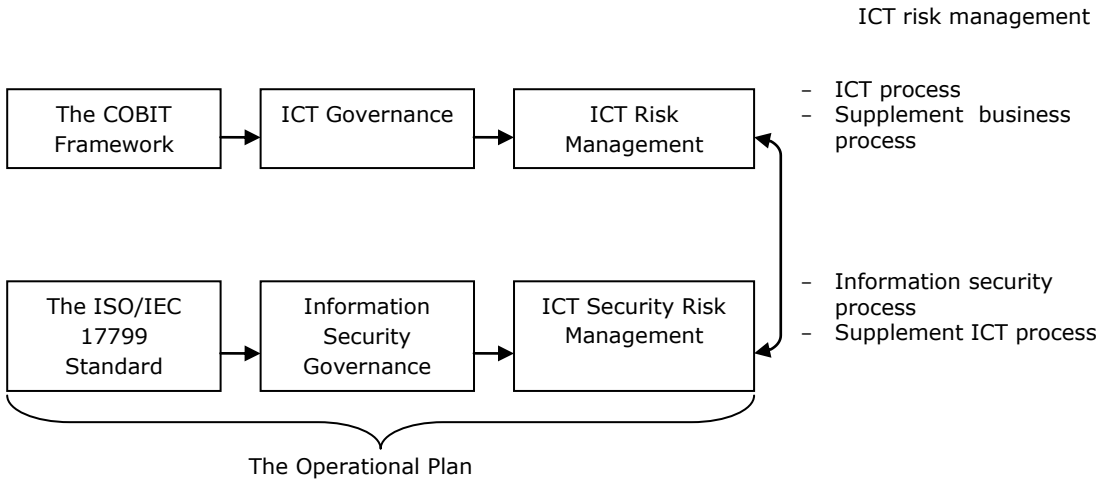


Figure 4-12: Control process: Case study B

Technology and systems

The interviewees noted that this organisation requires an appropriate risk management plan for dealing with the particular circumstances around an ICT problem. Risk assessment is important to identify uncertain events or risks before they happen. They argued that it is useful for unforeseen circumstances to be assessed when related to weaknesses in networks or data transmission. The probability and impact of this weakness is then evaluated as high, medium or low in order to prevent and mitigate such risk. In practice in this organisation, information security standards and policy must be planned in advance and implemented by updating usernames and passwords (i.e. access control), databases, software, back-up plans and back-up sites.

Generally, risks regarding organisational operations are classified as operational risk, credit risk or marketing risk within a banking institution, as noted by the Internal Audit Director. The respondents believe that risks related to ICT primarily are operational risks which must be prevented, mitigated or maintained at an acceptable level. Operational risk is associated with data accuracy, data reliability and data availability required to effectively serve customers of this organisation. For example, as mentioned by the Assistant Vice-President, data stored during the night shift must be appropriately handled and prepared for customer service the next day. If any events occur during the night, the organisation must be able to recover the data from this batch in readiness to serve customers. This implies that such circumstances are concerned not only with operational risk regarding ICT but also with ICT risk management processes and business continuity plan. Therefore, the ICT department focuses largely on access control of data, setting parameters for each operation system, routers and even firewalls. ICT control and audit

are then used to function as ICT risk management in this organisation. In this regard, the Division Director (ICT) revealed:

> *"I think … dealing with ICT risk, we define the origin of ICT risk in ICT and technical terms such as security in order to prevent the opportunity and to mitigate the impact of ICT risks by focusing on the setting configurations of hardware and software, ICT management and security management."*

4.3.5 Organisational ICT strategy

This organisation was in the process of detailed ICT risk management planning when the interviews were conducted. The Assistant Vice-President noted that at the initial stage it is necessary to define and develop a clear plan for ICT risk management. He believed that to provide a clear plan, senior management is responsible for three main areas: (a) defining policy, (b) defining processes, and (c) defining the technical approach (Figure 4-13). Although the technical approach might appear to be less the responsibility of senior management in so far as senior management is not familiar with the technical aspects of security ICT, it still needs to be covered in the corporate plan. This is imperative, the respondents argued, because this organisation needs to communicate with its customers, vendors and even competitors (i.e. third parties) via the internet or World Wide Web (WWW), and technical risk or security risk may emerge during such communications. As a result, the technical approach to security ICT must be the concern also of the corporate level and not the operational level alone.

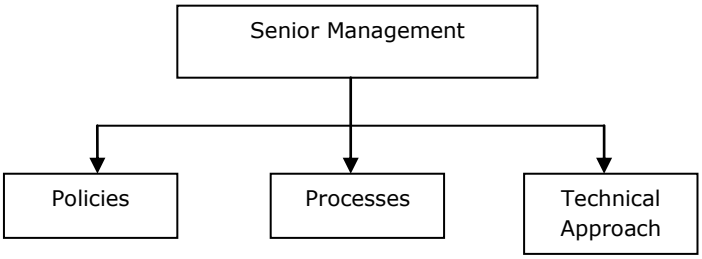


Figure 4-13: Roles and responsibilities of senior management: Case study B

The main responsibility of the ICT function regarding risk management lies with a technical approach towards information security management (ISM) in this organisation. The Assistant Vice-President added that ISM must cover business continuity management (BCM) and information security policy. BCM is focused on how to rapidly recover ICT systems and data from external and internal environmental impact. As a result, a disaster recovery plan (DRP) has been developed as part of the operational (action) plan for the business continuity plan (BCP) in BCM. The BCP is used to describe the details of how to recover the system when ICT risk from either an external or internal

environmental impact has interfered with organisational systems or data. The best practice standard for dealing with such a situation, The interviewees believe, is the ISO/IEC 17799 standard. This organisation plans to follow this standard to define BCM relating to ICT risk management.

Information security policy does not yet cover ICT risk management at the corporate level of this organisation. In contrast, ICT risk management is embedded in the operational (action) plan for each activity in the organisation. ICT risk management will be raised in the organisational policy area at the corporate level plan in the next few years because it has become an imperative issue for Thailand's business community. The organisation plans to define its ICT strategy by focusing on compliance as the first step. Compliance leads to ICT policy and is driven by the ICT security department through entire functions and/or departments in the organisation. Each function or department must now review its own processes against the regulatory and compliance tenets of the organisation. In so doing, each function and department must now assess its own risks as part of an ICT self-assessment process. This organisation considers that ICT risk management is relevant to general ICT, ICT application, and ICT security simultaneously.

4.3.6 Summary

The key factors addressed by, and which were the focus of, ICT risk management in this organisation were:

- policy;
- management of ICT resources;
- human resource management and planning or the management of people and their behaviour in the organisation;
- information security management; and
- ICT risk management planning.

Policy for ICT risk management is focused on three main areas (business, ICT and IS) in this organisation. This organisation defines business policy in alignment with ICT process. Creating ICT policy is focused on the BCP to rapidly recover ICT systems once they are down. A BCP is a major focus because it is vital that the services of a banking institution are up-to-date and real-time activities. While this organisation was not yet concerned with setting Information security policy at the time of the interviews, the interviewees mentioned that the organisation is intending to develop Information security policy at the

next stage of ICT risk management planning. The organisation has a risk statement which is representative of its policy approach to dealing with risk management.

Management of ICT resources is also the main focus in this organisation. Management of ICT resources is defined as general control in this organisation. General control includes the management of ICT infrastructure such as the software in ICT applications, networks, and operating systems.

Human resource management and planning is taken for granted as a key factor behind planning ICT risk management in this organisation. This organisation believes that education and training programs are essential, not only for operational staff but also for senior management. These programs help declare clear roles and responsibilities for all staff in relation to dealing with ICT risks. Moreover, education and training programs relate to the topic of the human resources authorisation process; compliance; and rules and regulations that all staff must follow.

Information security management is seen as another key factor in this organisation for dealing with ICT risk management planning. However, the interviewees did not clearly define their understanding of information security, but did mention that it is relevant to a technical approach such as the configuring of ICT infrastructure and systems or setting parameters for operation systems, routers and firewalls.

Lastly, linking practice in this organisation to the research purposes, a bottom-up process is the main method for driving operational activities around ICT risk management. In other words, ICT risk management planning is defined at the operational level first. Then the operational plan is communicated to the senior management level for revising, and to gain a consensus agreement on ICT risk management planning. From this point of view, the key factors in this organisation directly affect operational level planning and indirectly affect the corporate level plan to establish successful ICT risk management.

4.4 Case study C

4.4.1 Organisational profile

This organisation is the Thai branch of one of the world's largest international multimedia news agencies. Its services derive from financial services business through the internet. The Thai branch is a hub of software development. The core business strengths of the Thai branch lie in providing the content, analytics, trading and messaging capabilities required by financial professionals. In regard to digital communication, this branch has a wide range of ICT facilities to provide valuable information to its customers. With

substantial investment in ICT, this organisation views ICT risk management in terms of dealing with several types of ICT risk.

4.4.2 Organisational structure

Roles and responsibilities

The Technical Director revealed that the Thai branch is the headquarters of software development within Asia in the area of product services such as financial information and market data. The Technical Director added that ICT risk management in software development normally relates to risk management of particular projects rather than risk management as a whole across an organisation (Figure 4-14). In this organisation, two types of ICT risk management have been defined: one at the organisational level and one at the project management level. ICT risk management is planned by the holding company, at the corporate level, in the United Kingdom (UK). The ICT risk management plan is then delivered to all hubs around the world, to which they all must comply. Therefore, the hub in Thailand focuses on only the project management level of ICT risk management. Moreover, this hub plans its own risk management methodology regarding project management.

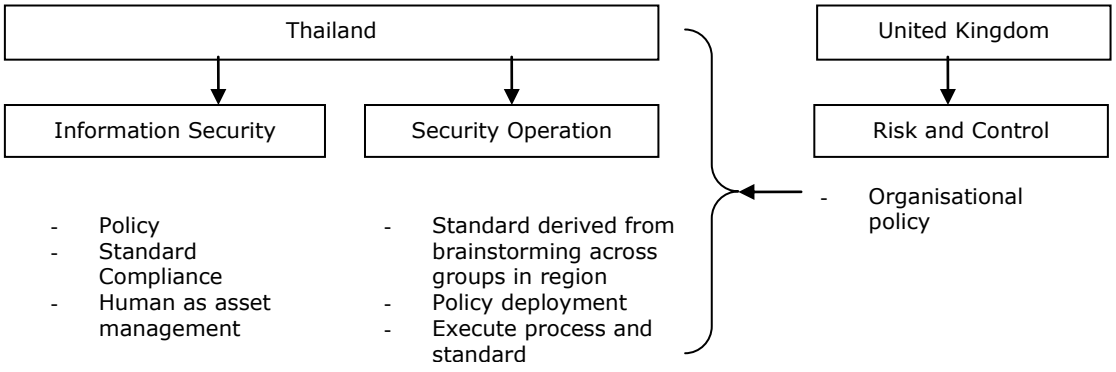


Figure 4-14: Roles and responsibilities: Case study C

According to this software development organisation, ICT risk management is an operational activity which requires a separate action plan from service lines such as business function, service function, ICT function and security function. Generally, risk management related to ICT has a well-defined plan at both the organisational level and the functional level, but this branch only focuses on the functional level.

The functional level of ICT risk management is understood in this organisation as information security risk management. Information security risk management covers information security, security operations and risk management. Information security and security operations are performed in Thailand but the risk management operations are only carried out in the UK. The risk management operations can be revised in response

to the management perspective—for example, at the time the interviews took place the focus was on governance. However, risk management penetrates all the functions of information security and security operations at the functional level or the operational level. Moreover, ICT risk management is also treated in the internal audit department of the umbrella organisation in the UK. Internal control and audit in Thailand is conducted once a year by focusing on all types of risk including human, operational, processes and ICT security.

The Technical Director explained:

> *"My organisation here in Thailand doesn't have a committee to be responsible for such ICT risk but we do have ICT risk management in each project."*

The Software Development Manager added:

> *"My organisation has ICT risk management in the software program itself; once we create software there are several criteria that we need to put into the system in order to protect, prevent and mitigate the risk."*

This organisation manages ICT risk management as a process of cooperation among the regions. The reason is that each region is responsible for different issue around the world, so that every rules and regulations are settled at the regions and then are forced to other branches in the region to follow. For example, it deals with ICT risk, especially securities, by cooperating with China, Singapore and Thailand (Figure 4-15).

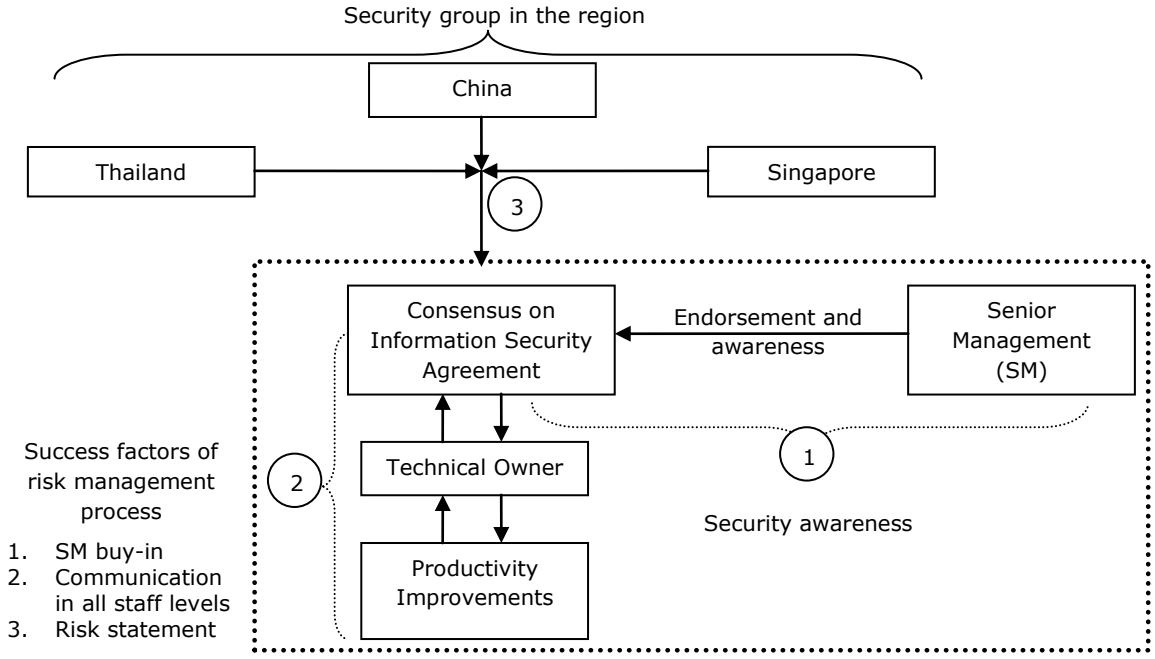


Figure 4-15: Information security process of cooperation among the regions: Case study C

For this organisation, the factors that lead to successful ICT risk management consist of endorsement by senior management and effective communication and development of risk statements. Endorsement by senior management is a major factor that can be seen as a consensus plan among the regions regarding security in ICT risk management. Communication entails two-way communication—thus both a top-down and bottom-up approach to ICT risk management—that draws on the intentions of both senior management and operational staff to incorporate information security into the corporate plan of this organisation. Lastly, the risk statement is included in the corporate plan in order to direct employees to work according to sound ICT risk management guidelines throughout the organisation. By doing so, this Thai branch uses the ISO/IEC 17799 standard to guide information security in ICT risk management.

ICT risk management treatment

ICT risk management is normally treated in any real detail at the functional level in this organisation. The functional level divides ICT risk management into two primary responsibilities (Figure 4-16).

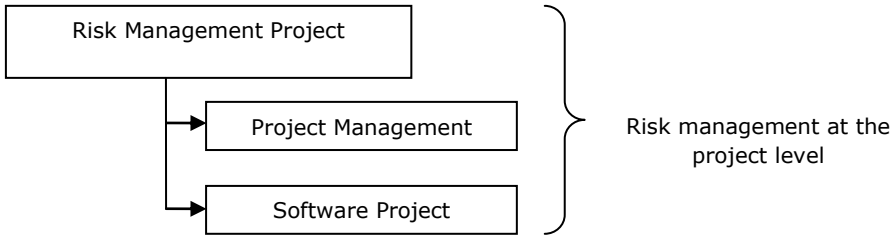


Figure 4-16: ICT risk management treatment in functionality: Case study C

Firstly, project risk management related to ICT aims to monitor the delivery of the project and the responsibility of the project developer. Secondly, software project risk management relates to how best to set particular functions and features in each software product in line with customer requirements.

According to project risk management, the project team seeks the agreement of stakeholders or clients/customers in order to set priorities for the risk management processes for the ICT project (Figure 4-17).

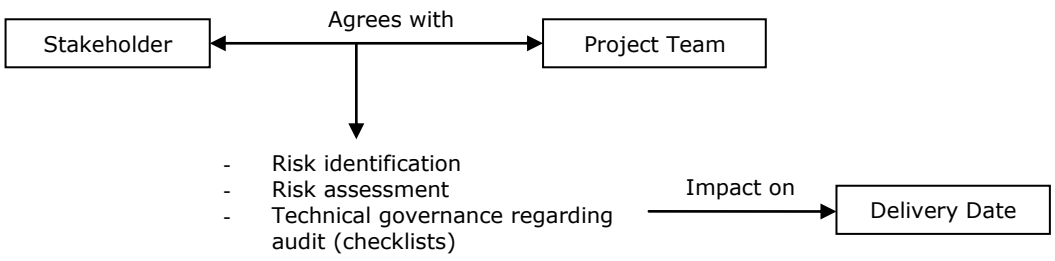


Figure 4-17: Software project risk management: Case study C

The Technical Director stated that:

> *"My work is all about creating software to serve our customers; therefore, we treat ICT risk management as project-by-project or job-by-job or job-order instead of as a whole organisation. Therefore, we focus on only clients' needs and requirements."*

4.4.3 Organisational process

ICT risk management instrument

The ICT risk management instrument used in this organisation includes risk assessment processes and risk management. The risk assessment process consists of a review of the security design, a review of security implementation and an assessment of operational security. Each process is written in a risk statement to guide staff to perform their roles accurately.

Risk management methodology covers escalation, tracking, reporting and exception handling as shown in the risk statement of this organisation. Moreover, this organisation has outlined clear responsibilities for its staff to manage risks at each stage of the lifecycle (Figure 4-18). The Information Security Manager explained:

> *"We deal with ICT risk by using software to capture and prevent the risk; we mainly focus on the ISO/IEC 17799 standard embedded in the software creation."*

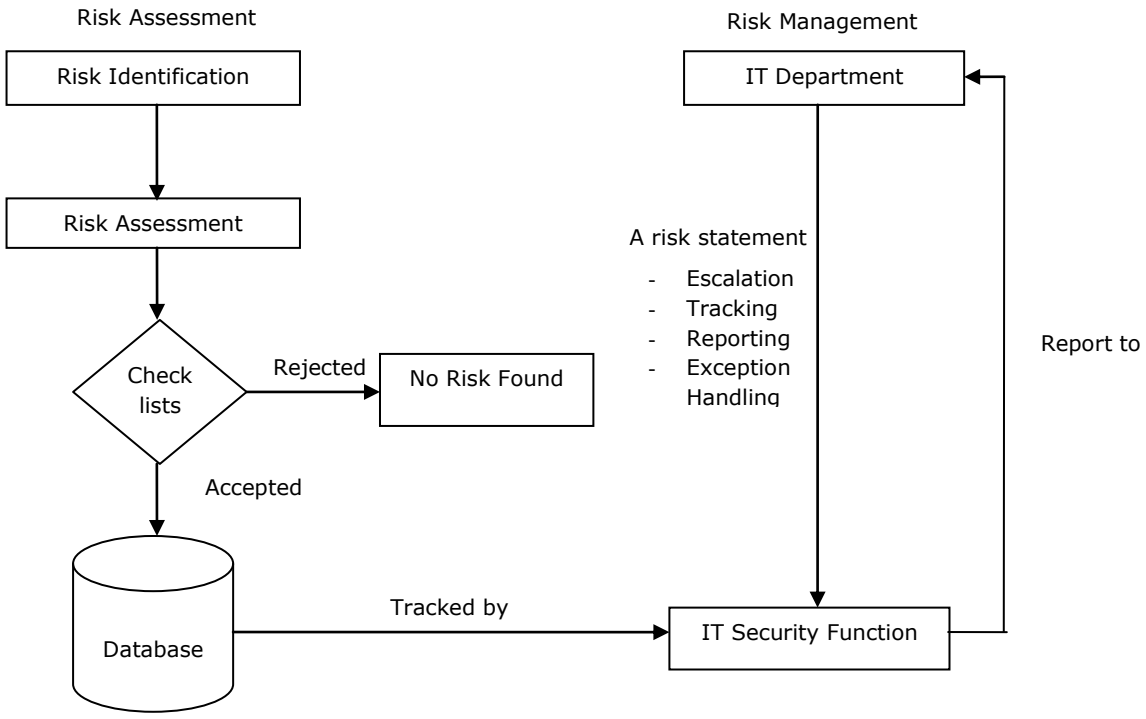


Figure 4-18: Risk management methodology embedded in software development: Case study C

This organisation uses its instrument, software risk management, to manage ICT risk. There are two components to software risk management: risk assessment and risk management. Firstly, risk assessment starts with risk identification. Risk identification is performed by each group of software developers. Whenever a problem occurs (e.g. error coding), a group of software developers or a software developer assesses the impact and the likelihood of each occurrence by checking the particular problem against current records in the database. The identified problem or issue is recorded in the database, which can then match the problem with former similar problems in the data. If there is little impact on the development process, the result will be shown as no risk found, and the problem or issue can then be rejected. In contrast, if the impact of a particular problem is found to be significant, it is stored in the database for the purposes of improving the process of software development in future. After that, the new problematic issue is tracked by IT security department where move the problematic issue to the risk management stage.

Secondly, risk management begins within the IT security department in this organisation. The IT security department retrieves the problem or issue from the database to report it to the IT department. The IT department then evaluates the problem in four stages:

- The escalation stage is to assess the level of risk occurrence for each problem or issue including whether or not it might occur repeatedly;

- The tracking step aims to identify the severity of risk impact for a particular problem or issue, and to provide recommendations to ensure staff are aware of the potential impact;

- The reporting step is to provide planned actions to mitigate the particular risk regarding the problem or issue and also to stipulate 'who' is responsible for this risk; and

- The exception and handling step is to take action in the IT security department on the risk regarding the problem or issue.

ICT risk management process

The ICT risk management process in this organisation is embedded in each project. Each project is controlled and audited by using software as a form of ICT risk management to record all the operation system processes in the organisation.

Firstly, the organisation conducts a review of security design which focuses on design and compliance with security standards, especially the ISO/IEC 17799 standard, and provides a checklist for security policy in order to maintain the integrity of information and prevent risk occurring as a result of incorrect ICT usage or ICT abuse.

Secondly, this organisation conducts reviews of security implementation which include checklists of non-design matters related to information security, such as penetration testing and initial system set-up, to ensure that particular functions or projects are secure.

Lastly, the assessment of operational security in this organisation focuses on identification of vulnerability, and thus the management of the potential for new risks to occur. After following the three steps of the risk assessment process, all risks are captured in each step and described using common terminology. Then all risks are recorded in the security risk database which is part of the organisational system that forms part of the risk management methodology.

The Technical Director explained:

> *"Our organisation provides the ICT risk management process in a risk statement that all staff levels can easily follow. A risk statement consists of the review of security design, the review of security implementation and the assessment of operational security."*

The Information Security Manager added:

> *"Our statement has a clear plan of what we must do step-by-step."*

4.4.4 Organisational control

Human resources

The primary focus of organisational control in organisation C is human risk, as the first priority of the organisation which strongly affects business function rather than service and security functions, because one third of software development staff are located in Thailand. At the time of writing, the organisation is facing a high rate of staff turnover. To control and prevent this, the organisation is offering incentives to encourage staff to work in a more positive environment and a training program to allow staff to rotate their position to assume different responsibilities, and thereby learn new skills. In this regard, the Technical Director stated:

> *"I think human resources are important for us due to we are software development; therefore, they are the first priority that we need to focus on."*

The Information Security Manager said:

> *"Staff is main person that may let the risk happening in the organisation; so they have to be controlled first."*

Control Process

Risk management control in this organisation is not concerned solely with the security perspective but also with business function, service function and security function (Figure 4-19). These functions are controlled from different perspectives. However, the main aim of each function is to meet the business objectives and goals. These organisational objectives and goals are to serve both internal and external environments. Therefore, the participants believed that it is imperative that each function is controlled properly.

The Technical Director asserted:

> *"According to software development, we have to focus on the business direction and internal direction; business direction is about business itself and services, internal direction is about security function or ICT function."*

The business function in this organisation is controlled by focusing on the management program which views human resources as having the main impact on business function. Furthermore, the service function is controlled by a focus on the operations program, which includes communication links as the main business process that serves customers and clients. Lastly, the security function is controlled by focusing on risk security project management which is included in software production on a job-by-job or job-order basis.

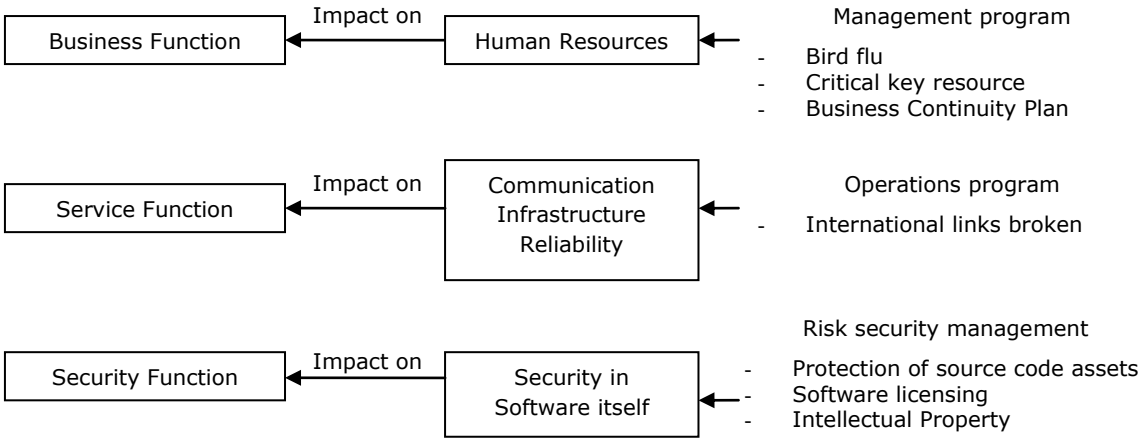


Figure 4-19: Risk management control: Case study C

Technology and Systems

In relation to technology and systems, there are two primary areas that are controlled in this organisation. The first priority of technology and system control is communication infrastructure reliability as a service function. The main service function involves running and feeding real-time information related to market data and financial information to customers via a communication link (i.e. CAT telecom, a public organisation in Thailand). If this communication link crashes, the service function is totally affected, akin to the

consequences of the earthquake that occurred in Southeast Asia in December 2006. Thus, the organisation has set this as the first priority for service function.

The Technical Director claimed that:

> *"Technology and system is very important because we are dealing with digital communication to feed our information to our customers; therefore, we are concerned about our communication link."*

Risk security management is also a major focus with the aim of protecting source code assets of the organisation's software, software licensing and intellectual property.

4.4.5 Organisational ICT strategy

The organisation includes an ICT risk management plan in its corporate (or annual) plan because the main business process focuses on project management (Figure 4-20). Therefore, ICT risk management constitutes the main section in the corporate plan that deals with ICT risks. Moreover, the organisation establishes ICT risk management plans at both the organisational and operational levels. The organisational level lies with the management plan, which includes organisational activities and personnel management. The operational level involves specific functions like project management and security project management. The Technical Director explained:

> *"We are not focusing on the organisational level plan regarding ICT risk management because our main process is dealing with job-order or job-by-job. However, I think the optimal ICT risk management plan must be at both the organisational level and the operational level."*

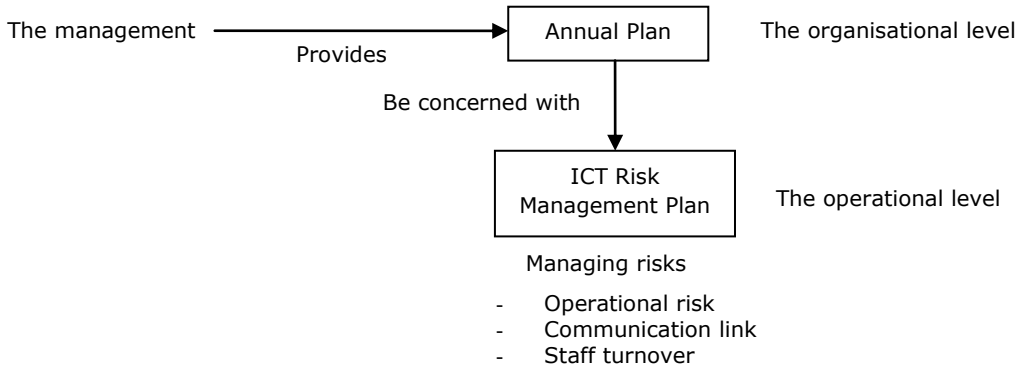


Figure 4-20: Requirements of ICT risk management plan: Case study C

In this organisation, the effective performance of information security must be separated from the ICT department and be reported directly to the Chief Executive Officer (CEO), the ICT audit committee (ICT perspective) and the audit committee (business

perspective) (Figure 4-21). The ICT department and ICT security function must have clearly defined and different responsibilities to each other. The ICT department is responsible for ICT operations such as ICT infrastructure, software, operating systems and networks. ICT security function should include security functions such as security policy, network security, security compliance and physical security.

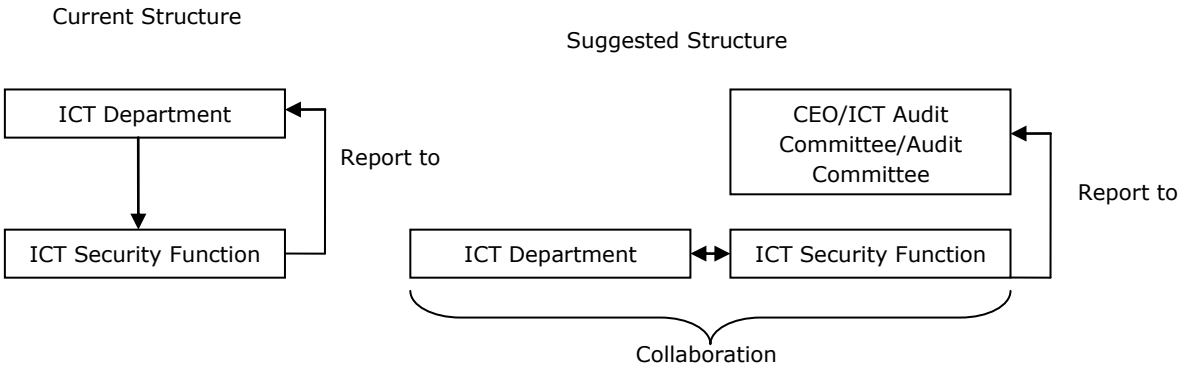


Figure 4-21: Separation of the roles and responsibilities of ICT and ICT security: Case study C

The Information Security Manager stated:

> *"I think ICT strategy should be reconsidered and the effective way of both ICT management and ICT security must be separated and directly reported to management because the main focuses of both are different, although they are in the same area."*

4.4.6 Summary

The key factors addressed by, and which were the focus of, ICT risk management in this organisation were:

- policy;
- human resource management and planning or the management of people and their behaviour in the organisation;
- information security management; and
- ICT risk management planning.

Policy for ICT risk management is focused only on information security policy which aims to maintain information integrity of software created by this organisation. The organisation's risk statement is also a concern within organisational policy because when creating software it is imperative that staff follow organisational rules and regulations in order to prevent, avoid and mitigate ICT risk in project management.

Human resource management and planning are of major concern because staff in this organisation are creating software for its clients. This key factor is based on the delivery of training programs, human resources protection and human resources security.

A central focus of information security management in this organisation is that this function is embedded in the software created. IS management includes asset management which covers software and the protection of source code assets.

Lastly, linking this organisation's practice to the research objectives, ICT risk management planning occurs at the operational level. The operational level plan is relevant to operational activities with regard to developing software in this Thai branch. As a result, a bottom-up approach is used to control the operations by managing software risk in project management. Therefore, this organisation is concerned with information security policy, human resource management and IS management and their effect on the operational plan which in turn impacts on successful ICT risk management planning.

4.5 Conclusion

This chapter has presented a discussion of the current profile of ICT risk management in organisational practice for the case study organisations A, B and C. It is evident from the respondents' views that ICT risk management is conducted in relation to the areas of organisational structure, process, control, and strategy. Each of these elements of ICT risk management is discussed separately below.

Organisational structure

Firstly, ICT risk management is governed by a separate committee which is responsible for different tasks in the organisation relating to ICT risk management. Case study organisation A has the clear responsibility of setting the ICT risk management strategy by monitoring and directing internal processes in the organisation. The audit committee mostly directs and monitors the internal operational transactions. The risk management committee is mainly concerned with several types of risk including business and ICT. Risks that occur as a result of information security problems are governed across the entire organisation by an enterprise-wide security committee. In this organisation several types of risk—including operational risk, business risk, ICT risk and IS risk—can be mitigated against, avoided and prevented simultaneously. By contrast, the organisations in case studies B and C were concerned less with allocating the responsibility for dealing with ICT risk management.

Secondly, the position level of ICT risk management is considered in all three case studies, but in each case from a different perspective. The organisations in case studies A and B control and audit ICT risk at both the corporate level and the operational level appropriately because ICT risk management covers the origin of risk and the risk impact. This helps the department report back to the Board of Directors who will then outline the process of risk treatment for the other departments. The organisation in case study C is different from organisations A and B because it is a software hub. The major tasks of its operations lie in computer programming or software development; as a result the process of risk treatment is in the application software embedded in each project produced.

Thirdly, the component of ICT risk management comprises ICT control and audit as well as information security control and audit. According to organisations A and B, ICT risk management relates to ICT activities and information security activities when dealing with ICT risk. Both organisations brief about the term of ICT activities in ICT policy and the term of information security activities in Information security policy. This means that the staff understand their roles and responsibilities when facing any type of ICT risk incident and that they must report such occurrences to the board. In contrast, organisation C focuses only on the IS part because the work of its staff is entirely dependent upon software development. Therefore, the staff in this organisation always react to a risk by using the application software to fix the problem and mitigate against the negative impact.

Organisational process

Firstly, the risk statement is seen from a different perspective according to the position level. However, the details included in the risk statement cover the process for both the entire organisation and the specified functions in the organisation. In organisations A and B, the risk statement is viewed as an ICT risk management instrument for the staff to follow at the corporate level and at the operational level. With regards to the meaning of the risk statement at both levels, ICT risk management is used to clarify the risk methodology in the corporate and operational plans. For example, in the corporate plan senior management in the organisation sets the overall scope of ICT risk management. Furthermore, in the operational plan, the organisation outlines the details of ICT risk management processes aligned with the corporate plan. This is a clear process statement for dealing with ICT risk in the organisation. Conversely, organisation C mainly focuses on the specific function of each project, which means that the organisation is concerned more with the operational level than the corporate level.

Secondly, in order to specify the processes in the organisation, organisations A, B and C all follow the guidelines from the internationally accepted framework and standard of

COBIT, of ISO/IEC 17799 and of enterprise risk management (ERM). Organisation A complies with the COBIT framework and the ISO/IEC 17799 standard to specify the appropriate processes for ICT management for both the corporate top-down approach and the operational bottom-up approach. On the other hand, organisation B is concerned also with aligning COBIT with ERM, as the methodology for business risk management in the organisation which is implemented from a business angle to direct, control and monitor ICT. This organisation mainly focuses on a top-down approach as the main approach taken at the corporate level, whose directives are communicated to the operational level. Organisation C considers only information security to be part of a bottom-up approach to ICT risk which it sees is the natural concern of the software development side.

Organisational control

A common concern among all three case study organisations is the effective control of people, process, technology and systems. The three organisations concentrate on the control of business, service, ICT and IS functions simultaneously, although they emphasise these four functions from different perspectives. Because they are different types of organisation, each controls and monitors the transactions generated from internal sections and external sections in different ways. For example, in organisations A and B, the entire transaction process relates to the operational process from working routine and billing actions with customers. Thus business, service, ICT and IS functions are monitored concurrently. On the other hand, organisation C operates each software development project on a job-order or job-by-job basis which leads to ICT risk management being carried out also on this basis, and focusing on application security management. Hence, the framework and the standards are considered in isolation with each project to achieve ICT risk management in this organisation. However, service functions, including those involved with both internal and external parties, remain unaddressed in organisation C. Furthermore, service function is not mentioned in detail in this research because it relates to another standard of ICT service management called the Information Technology Infrastructure Library (ITIL).

Organisational ICT strategy

Consideration of the organisational ICT strategies of the three case studies illustrates that they focus on ICT risk management in different ways. However, the case studies highlighted some common issues (i.e. top-down and bottom-up risk management approach) that an organisation should consider in relation to ICT strategy. Furthermore, both top-down and bottom-up approaches are considered relevant depending on the type of business, and this can be clarified when an organisation commences ICT risk management planning. An organisation should consider risk planning at the corporate

level within an overall ICT plan, which then translates into the operational plan by covering both ICT management and IS management. ICT risk management is considered at both the corporate and operational levels as ICT risk management and ICT project risk management respectively. Moreover, different management levels in the organisations under study were concerned that the plan should be revised at both levels to reach consensus agreement on the final plan. This means that ICT risk management is planned at the corporate level as the scope of ICT risk management which then drives the operational level to plan ICT project risk management in detail within each relevant department. However, both ICT risk management and ICT project risk management should be planned in the same direction as part of an entire organisational ICT risk management plan. As a result, successful ICT risk management planning focuses on collaboration between management level activities and operational level activities in order to deal with ICT risks successfully.

According to the four components, the key factors that determine successful ICT risk management in each organisation emerged in the interviews. The key factors in case studies A and B are policy; management of ICT resources; human resource management and planning; information security management; the corporate level plan; and the operational level plan. Similarly, case study C considers that policy; human resource management and planning; information security management; and the operational level plan are the key factors.

As a result, ICT risk management in case study organisations A, B and C is focused at both the corporate and operational levels. The corporate level sets the overall ICT risk management plan, while the operational level sets the specific technical security plan for ICT. Furthermore, respondents from both the corporate and operational levels in the three organisations revealed that policy; human resource management and planning; information security management; and management of ICT resources are the key factors to consider when dealing with successful ICT risk management. The next chapter presents the other three case studies D, E and F, and considers the operations of ICT risk management in both their own organisations and that of their clients.

Chapter 5

CASE STUDIES IN THAI BUSINESS ADOPTION OF ICT RISK STANDARDS: CASES D-F

This chapter reports on the practice of ICT risk management in Thai organisations from both the organisational and consulting perspectives. The chapter begins with a discussion of the ICT risk management profile of the case study organisations D, E and F. The qualitative findings of the case studies D, E and F are then presented next. The conclusion of all case studies A, B, C, D, E and F are then presented in the next chapter.

5.1 Case study D

5.1.1 Organisational profile

This organisation is an international consulting organisation which provides consulting services such as auditing advice, risk advice and corporate governance. This organisation is internationally and nationally recognised for its advisory services in the areas of business and ICT processes. ICT risk management was discussed in the interviews with the Chief Finance Officer (CFO) who is also the Chief Information Officer (CIO) and the ICT Advisory Director. The CFO/CIO explain ICT risk management in his organisation, while the ICT Advisory Director discusses ICT risk management based on his consulting experience with his clients.

5.1.2 Organisational structure

Roles and responsibilities

The ICT Advisory Director explained his view that setting the framework for risk management should include business risk and ICT risk, which are generally the responsibility of senior management. He added that senior management is not familiar with ICT risk management. He further explained that among his clients the larger organisations usually establish a risk management committee to take responsibility for setting a framework for business and ICT risk management (Figure 5-1).

The Chief Finance Officer and Chief Information Officer (CFO/CIO) supported the perspective of the ICT Advisory Director on the client organisations, adding that their organisation defines the main responsibilities of a risk management committee which include setting a risk management framework that addresses policy, responsibility, definitions of risk and acceptable risk levels. The CFO/CIO also stated that a framework for risk management that consists of both business and ICT perspectives is defined as enterprise risk management (ERM).

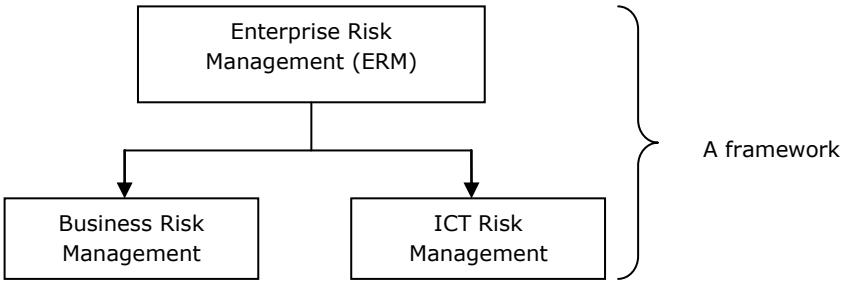


Figure 5-1: Roles and responsibilities: Case study D

Based on his consulting experience, the ICT Advisory Director pointed out that departments in his client organisations normally understand that risk management is the sole responsibility of the risk management unit or department. He added that risk management is performed in all of his clients' organisations in order to prevent, mitigate and avoid risks in both business and ICT. He further noted that in these client organisations, the roles and responsibilities of staff are classified into three types: doer, facilitator and reviewer. The doer is simply the management or staff employee who performs their normal functions. A facilitator is a person who monitors staff performance to ensure it abides by the organisation's framework. A reviewer is an independent role chosen from among the doers or facilitators who reviews all processes in a framework such as the way in which ICT risk management acts to define objectives, identify risk, assess risk or respond to risk. The ICT Advisory Director suggested that*:*

"Risk management is a responsibility of staff that is classified in terms of doer, facilitator and reviewer in my clients' organisations."

ICT risk management treatment

From the consulting perspective of the ICT Advisory Director, before dealing with ICT risk management, his clients' organisations must formulate an ICT risk management framework to provide the necessary guidance. Such guidance is offered by the main framework of enterprise risk management (ERM) which outlines the methodology for dealing with risk management, including business risk and ICT risk. For example, without a framework, departments in his clients' organisations may not identify or define ICT risk and risk management in the same way due to divergent interpretations and perceptions. Consequently, his clients' organisations require a framework to deal with ICT risk management that is consistent across all departments in his clients' organisations to target the same goals and objectives. A framework is formed through consensus among all management levels.

The CFO/CIO compared the practices of client organisations with his own organisation that this organisation has a framework called the 'baseline' which is normally set every year at a regional level called 'a global plan' (e.g. in the region of Asia), which delineates the responsibilities of branches in each country. The baseline in this organisation is controlled by the ICT security group who not only monitors and complies with the operational and security functions but also defines business policy and security policy.

Components of ICT risk management

The ICT Advisory Director noted that his clients' organisations separate the responsibility of ICT function into ICT application and ICT security; staff can then manage ICT risk appropriately and successfully. In essence, the ICT Advisory Director mentioned that ICT application and ICT security are imperative for coping with ICT risk management, yet they are managed independently. In this regard, he stated that:

"My opinion is that we should well clarify what ICT means and consists of because this will help us clearly control it or them appropriately. From my point of view, ICT function includes ICT application and ICT security."

5.1.3 Organisational process

The ICT Advisory Director revealed that in his clients' organisations ICT risk mostly relates to operational risk which penetrates into all areas of operational process. Therefore, he describes the main components of ICT risk management in these

organisations as incorporating and defining: (1) the ICT risk management process; (2) the ICT structure; (3) the roles and responsibilities of each department in dealing with ICT risk management; and (4) how to monitor ICT risk management as noted by ICT Advisory Director.

The ICT Advisory Director further suggested that the ICT risk management process in his clients' organisations is classified into three types: advanced, semi-advanced and normal plans. From his point of view, advanced is defined as a well-organised plan; semi-advanced refers to a plan that is beyond a standard but has not been perfected; and normal is a plan that is equivalent to a risk management standard.

The ICT Advisory Director stated that, in the advanced performance plan, the ICT risk management process is embedded into organisational objectives (Figure 5-2). The ICT Advisory Director added that his clients' organisations classify: (1) which risks related to ICT will impact on business and ICT objectives; and (2) what impacts will be an obstacle to achieving business and ICT objectives. Both must be outlined in the business and ICT strategy in the corporate plan, as well as what actions can be adopted to prevent, avoid and mitigate business and ICT risks. The corporate plan will outline the processes in detail for long-term implementation over the next one to three years.

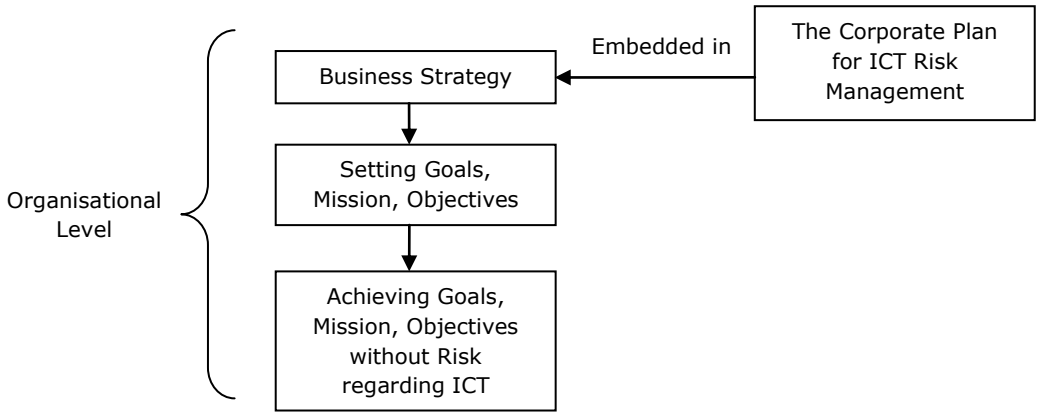


Figure 5-2: The advanced performance plan for ICT risk management: Case study D

The ICT Advisory Director further stated that, in the semi-advanced performance plan, his clients' organisations conduct a risk assessment, and then identify the control needed to 'fix' the risks identified. If ICT risk is found in the form of system hacking, control objectives will be found to resolve that particular problem (Figure 5-3). This event will be documented in order to determine how to deal with it as part of the operational plan but it will not be included in the business strategy within the corporate plan.

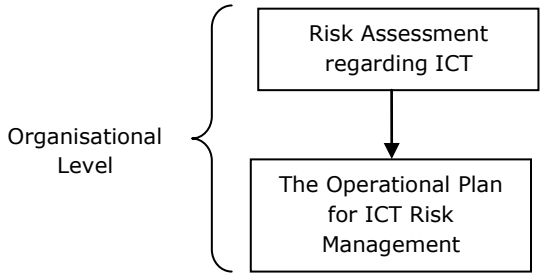


Figure 5-3: The semi-advanced performance plan for ICT risk management: Case study D

The ICT Advisory Director also explained that, in the normal performance plan, his clients' organisations manage their risks on a point-by-point basis, namely as functional risk management (Figure 5-4). This process is focused on the details of specific functions or departments; and each department manages its own risks in its own way and thus there is no organisational consensus. For example, security risk management of security systems is handled by the IT department only. This matter can be understood as ICT risk management on a project basis such that it is carried out project by project, as revealed by the ICT Advisory Director.

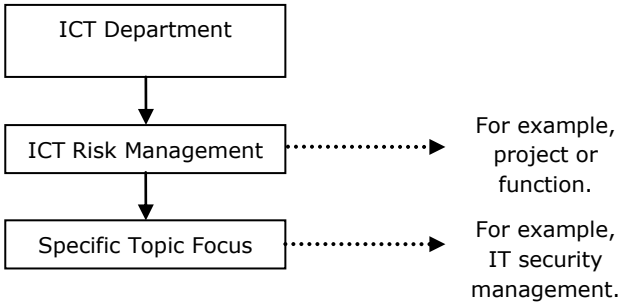


Figure 5-4: The normal performance plan for ICT risk management: Case study D

Nevertheless, the ICT Advisory Director believed that performing in the context of organisational consensus is the best way to deal with ICT risk management. In fact, risk management is the responsibility of all the departments and staff of his clients' organisations, to be monitored, treated, and reported on in relation to the impact on business and ICT processes. Thus, ICT risk management focuses on three elements in the context of an organisational consensus: people; process; and technology and system. It is also embedded within a strategic plan that forms part of the corporate plan developed through consensus among all management levels. After that, ICT risk management will be developed to cover both business function and ICT function. The results derived from the corporate plan can then be monitored and reported to the Board of Directors (BOD), in order to revise the methodology of the corporate plan to deal more successfully with ICT risk management. The Executive Director (ICT advisory) revealed that:

"From my long experience I saw several types of ICT risk management process (advanced, semi-advanced and normal plans) and I think that each of them is well suited with the type of business and direction."

5.1.4 Organisational control

Human resources

The CFO/CIO discussed ICT risk management in his organisation from an organisational perspective. The CFO/CIO said that the area of human resources is not managed properly in Thailand because of a lack of personnel privacy. Where the privacy of personnel in Western countries is strictly maintained as a priority, the nature of Thai culture does not necessitate this. According to the CFO/CIO, in Thai culture the concept of privacy means that something is private among close friends or family, rather than implying the protection of individual privacy. In this organisation, there are many nationalities who demonstrate no concern over this matter. The CFO/CIO further added that it can be difficult to control the confidentiality of information within human resources. In the context of Thai culture, therefore, privacy is not really a major concern but it is considered before developing organisational policy, particularly in an international company such as this one. Such consideration may help the organisation apply security policies more smoothly and easily.

The CFO/CIO further explained that the other area of concern in human resources is the potential for information leaks, where internal information may be taken out of the organisation without proper controls. Therefore, this organisation requires strict controls in relation to securing data by establishing security policy to monitor all types of organisational data and information.

The CFO/CIO added that ICT security awareness is another ICT security issue that may be influenced by Thai culture. Although Thai staff members understand the rules of security awareness, in general they do not think it is very important for them. In contrast to Western culture, based on the CFO/CIO's opinion, Thai staff members often ignore this issue and do what they want, unlike Western people who often seem to be concerned about pirated software, software licensing or intellectual property. Thus, in the Thai context these attitudes and behaviours may lead to the occurrence of ICT risk from ICT abuse and lack of awareness. With regard to ICT security policy, this organisation utilises software detection to monitor all types of software installed in the organisation's computers. Moreover, the organisation trains all staff about the potential risks from ICT abuses and displays its ICT security awareness program on sign boards around the office.

Control process

Based on his consulting experience, the ICT Advisory Director pointed out that the organisational control process adopted by his clients starts with defining the control objectives. His clients' organisations must define their business objectives by recognising the rationale for using ICT, what is required from ICT and what purpose is served by ICT. The business objective therefore is the crucial element for an organisation to consider. In this regard, the COBIT framework is used to set business objectives that align with ICT objectives. The ICT Advisory Director further revealed that the COBIT framework clearly defines the alignment of business goals to ICT goals in order to achieve the ICT criteria stipulated in COBIT: effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability.

The ICT Advisory Director stated that If ICT cannot make a business function efficiently and effectively, ICT risk will occur. Most ICT risks come from operations such as security risk, technical risk, financial risk and strategic risk. Thus, the ICT Advisory Director believed that his clients' organisations are concerned with the effectiveness of people, process, technology and system elements because this reflects the efficiency and effectiveness of ICT risk management.

The ICT Advisory Director additionally claimed that security related to human resources is linked to security awareness of staff in his clients' organisations. Security in relation to process is associated with adequate performance of the ICT risk management process. Security related to technology involves an appropriate security system in application and/or in ICT infrastructure. In light of the above, his clients' organisations must recognise the sources of ICT risk such as people risk, process risk and technology and system risk. In this way, his clients' organisations can find effective ways to cope with ICT risk through the adoption of useful frameworks or standards.

Comparing these practices with the practice in his own organisation, the CIO/CFO stated that the control objectives relating to the frameworks or standards in his organisation are focused on five main processes: a process of information systems management; a process of defining strategy; a process of security systems; a process of systems development and changes; and a process of business continuity management. The CIO/CFO noted that these five main processes are outlined in the COBIT framework and the ISO/IEC 17799 standard. The COBIT framework engages with the overall ICT control framework of an organisation. Other standards and frameworks such as the Information Technology Infrastructure Library (ITIL) are also considered in the organisational plan as ICT service management. The CIO/CFO revealed that:

"I think the main aim of an organisation is to utilise ICT enabling business process and ICT process efficiently and effectively; therefore, an organisation should focus on the heart of business and ICT elements which are internal and external environments: internal environment is data and information, people, and technology and system; external environment is services to customers."

Technology and systems

The CIO/CFO said that organisational control regarding technology and system elements in this organisation is presently focused on data retention, which includes the management of information security and data. For example, this relates to how the organisation retains its data when a computer has been replaced or how the organisation manages the destruction of data. These are the critical ways for dealing with data retention regarding ICT risk management in this organisation.

5.1.5 Organisational ICT strategy

The CFO/CIO recommends that organisational ICT strategy not be the concern of only the senior management level but also of operational staff. The CFO/CIO added that using the COBIT framework alone is not sufficient for dealing with ICT risk management. The ICT Advisory Director similarly claimed that the nature of the COBIT framework is to provide guidance for the organisation to follow overall ICT control (i.e. technology) but that it does not provide detailed direction like the standard. The ICT Advisory Director concluded that the COBIT framework should be used together with other standards or frameworks, such as the ISO/IEC 17799 standard, to cover overall ICT control and specific security control (Figure 5-5).

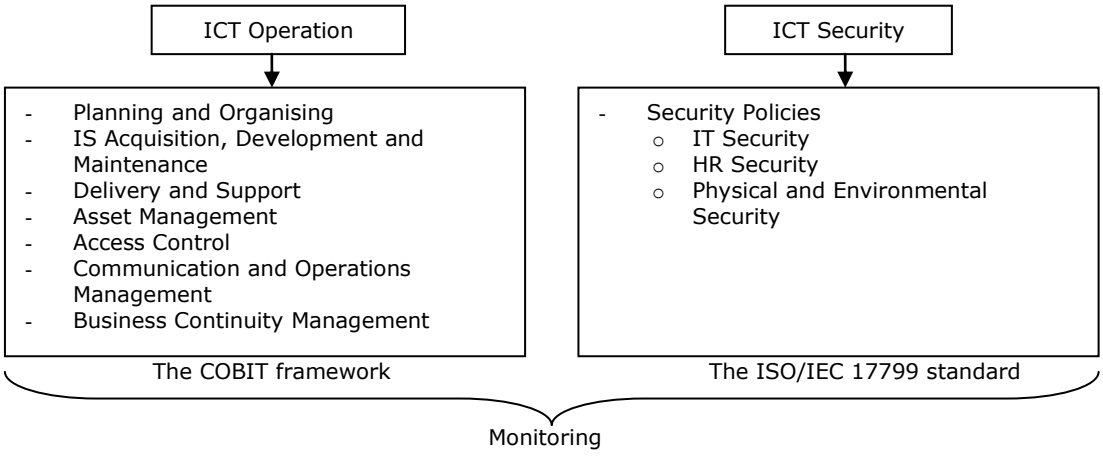


Figure 5-5: Suggestion for the selection of control objectives from the COBIT framework and the ISO standard: Case study D.

To apply both the COBIT framework and the ISO/IEC 17799 standard, the ICT Advisory Director suggests that his clients' organisations can select the most successful factors from each to deal effectively with ICT risk management. He revealed that COBIT is the framework that fits four criteria—people, process, technology and system—reflecting the real ICT risks. The ICT Advisory Director therefore concluded that the COBIT framework and the ISO/IEC 17799 standard ought to be of primary concern in ICT risk management. The ICT Advisory Director further noted that the COBIT framework is responsible for ICT operation and the ISO/IEC 17799 standard is responsible for ICT security. He explained that ICT operation includes planning and organising; acquisition and implementation; delivery and support; monitoring; asset management; access control; communication and operation management; and business continuity management. In contrast, ICT security covers security policy (e.g. technical security, human resources security, and physical security) and monitoring as explained by the ICT Advisory Director. Therefore, both ICT and ICT security operations are managed to put ICT risk under control, as described by the ICT Advisory Director.

5.1.6 Summary

The key factors addressed by, and which were the focus of, ICT risk management in this organisation and the clients' organisations, were:

- policy;
- management of ICT resources;
- human resource management and planning or the management of people and their behaviour in the organisation;
- information security management; and
- ICT risk management planning.

Policy for ICT risk management is defined in this organisation under the business, ICT and IS policies that are viewed from an organisational perspective in this organisation and from a consulting perspective in the clients' organisations. From the interviewees' point of view, ICT and IS policies are recognised to be the key factor to be considered when dealing with ICT risk management. Business continuity management is another element that is of significant concern in this organisation and in the clients' organisations.

The management of ICT resources is a key factor recognised by the interviewees in this organisation. The management of ICT resources is mainly based on the adequate provision of ICT application, software and ICT infrastructure to all staff levels.

Human resource management and planning includes protection and security of human resources that can be impacted by human error, and the provision of appropriate skills and training for staff.

The participants also highlighted that information security management is a major concern in terms of both technical risk and operational risk. This key factor is classified in terms of information security awareness and system security (e.g. data retention using software detection).

Lastly, linking these practice based on the organisational and consulting perspectives to the research purposes, it is evident that senior management and the operational managers must plan ICT risk management at both the corporate and the operational levels. Organisational policy; management of ICT resources; human resources protection and security; and IS management all directly affect both the corporate level and the operational level planning around ICT risk management.

5.2 Case study E

5.2.1 Organisational profile

This organisation provides a wide range of quality services such as audit, tax, financial and risk advisory services. The organisation helps firm clients improve their operational performance, mitigate risk and enhance value for both shareholders and stakeholders. Furthermore, the advisory services cover assisting firm clients to manage enterprise-wide risk management for corporate governance; restructuring of people management; and cross-border transactions to leverage ICT and intellectual assets. The Risk Advisory Services (RAS) group forms a major part of this service, which covers the following areas: governance, risk management and internal controls; environmental and social performance and reporting; and intellectual property and information systems. Moreover, these services are not only provided to clients but also constitute a major focus for this organisation internally.

5.2.2 Organisational structure

Roles and responsibilities

The Risk Advisory Director (RAD), who is also the Chief Information Officer (CIO), said that this organisation has assigned a risk management partner to be responsible for organisational risk management in the areas of business and ICT (Figure 5-6). The RAD/CIO further explained that organisational risk management is classified into two levels in the region (Asia-Pacific), covered by global and local risk management policy.

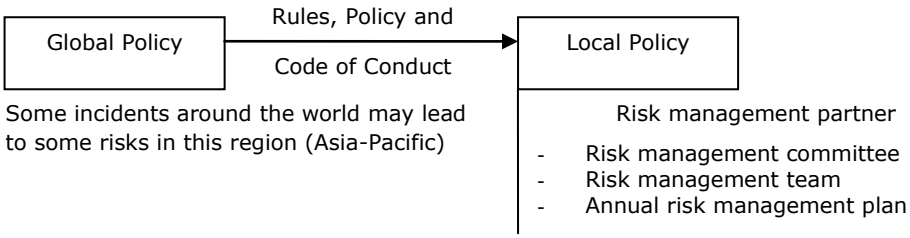


Figure 5-6: Roles and responsibilities within global policy: Case study E

Global policy is dictated by the holding organisation and implemented in all the regional branches around the world. Any change in global policy is normally precipitated by new incidents that impact on the organisation worldwide. In contrast, the main responsibility for local policy lies with senior management. Risk management is one critical part of this organisation which is handled by the risk management partner. The main role and responsibility of the risk management partner is to determine those people in the organisation who are responsible for dividing the risk management concerns (Figure 5-7). For example, this organisation has divided the responsibility for risk management between the management committee board and the audit committee.

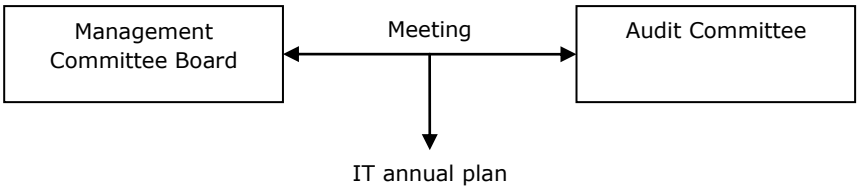


Figure 5-7: Roles and responsibilities within local policy: Case study E

The main roles and responsibilities in this organisation are normally classified into who, when and how criteria. 'Who' relates to a person or a group who takes responsibility for ICT risk in the organisation; 'when' involves the period of time during which action over particular ICT risks is to be taken; and 'how' is the treatment or process to be adopted for the particular event or circumstance. Therefore, this organisation sets the roles and

responsibilities for its staff to take responsibility for ICT risks. In this regard, the RAD/CIO explained:

> *"I think every organisation should define 'who', 'which group', 'which process', 'when' and 'how' to deal with risk technology."*

Components of ICT risk management

ICT risk management in this organisation covers two main areas: ICT operation and information security. ICT operation is identified by hardware, software and networks. In contrast, information security is related to user management, user account management, user authority, user rights, and security plans (i.e. personal firewall, filter spam and access control). ICT operation and information security in this organisation have to be set as organisational standards in order to prevent ICT risks cause by external impacts. For example, the organisation only provides a network port for its own computers; if any staff members bring their own computers (referred to as an 'unstandardised pattern') to work, the system will automatically lock and clean up that particular network port.

5.2.3 Organisational process

ICT risk management instrument

The RAD/CIO mentioned that ICT risk treatment is established at the corporate level every year. ICT risk treatment is known as security assessment in this organisation, which acts as the ICT risk management methodology that it uses to assess itself (Figure 5-8). This assessment generates a 'score', the details of which are provided to the global ICT security officer in the organisation. In so doing, the organisation gains an understanding of the weak and strong points in its systems and technology.

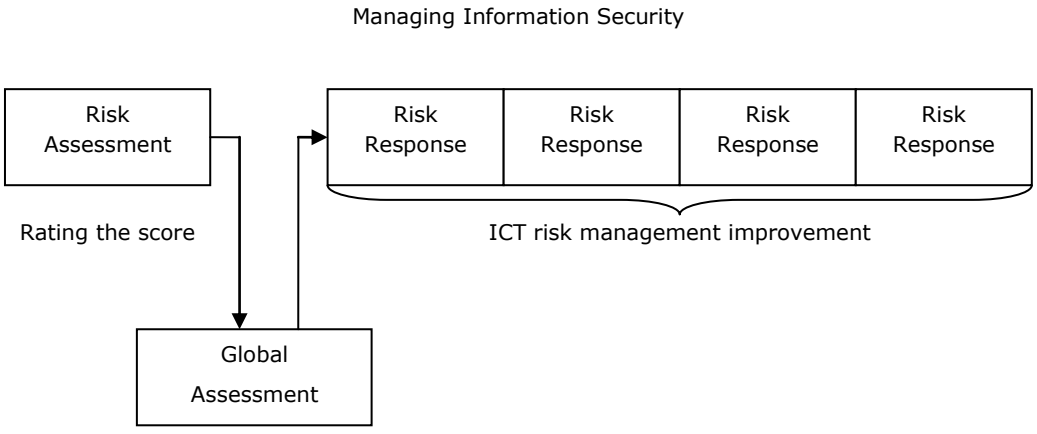


Figure 5-8: ICT risk treatment: Case study E

After rating itself through the risk assessment and sending this score to the global team, the global team comes to reassess this performance and to provide guidelines on dealing with the weak points to improve local plans and policy. From this point of view, the RAD/CIO mentioned that risk assessment (once a year) and risk response (about four months each year) regarding ICT risk management are more important than risk monitoring because they enable the organisation to increase or reduce the actions for dealing with ICT risk. However, the RAD/CIO also stated that the organisation still needs to improve its monitoring of risk in order to better manage ICT risk.

5.2.4 Organisational control

Human resources

The primary concern of this organisation is focused on the control of staff who lack awareness about the potential for unintentional breaches of the system. This organisation attempts to avoid operational risk by forcing its staff to sign an agreement regarding information security policy. This agreement acts to control human risk or operational risk, which can be difficult to control and protect. The RAD/CIO revealed that:

> *"My organisation has the policy to control human action in both positive and negative ways; every staff member needs to sign the agreement that can help my organisation protect technology, process and people."*

Control process

The RAD/CIO explained that the ICT risk management process in this organisation is classified into three main areas:

- Prioritising risk impact and the rating of risk potential as low, medium or high;
- Using risk management software to evaluate the risks; and
- Conducting an ICT security assessment using a balanced security score card based on the control objectives of the COBIT framework, the ISO/IEC 17799 standard and the Information Technology Infrastructure Library (ITIL) framework[3].

[3] The ITIL framework is a set of concepts and practices of Information Technology Service Management (ITSM) embedded in IT development and IT operations (OGC 2009). The main purpose of this framework is to help an organisation to deal with services in ICT process in order to improve customer services in both the internal and external environment (ITGI/OGC 2008).

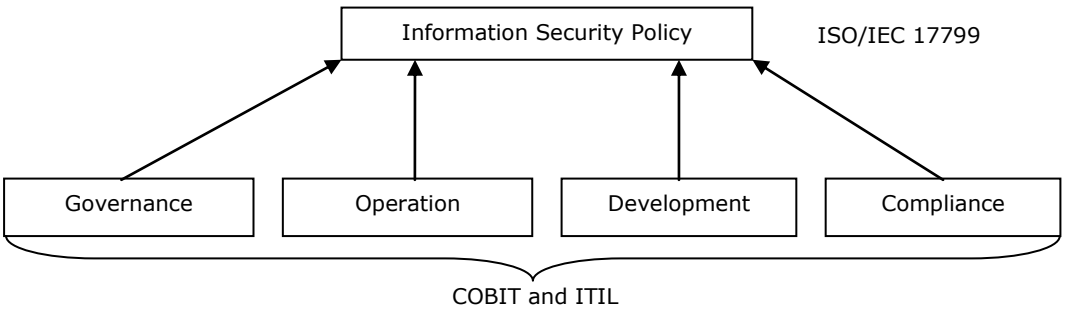
In this organisation, most of the criteria related to the above come from the ISO/IEC 17799 standard, while some derive from the COBIT and the ITIL frameworks in relation to the balance security score card.

Technology and systems

The RAD/CIO pointed out that recently the organisation had been focusing more on governance in relation to ICT and IS because these areas have become more critical to Thai business. The RAD/CIO added that the importance of ICT and IS governance has emerged from the introduction of a new Act in Thailand—the *Computer Crime Act (CCA) 2008*—which mainly focuses on human resources. ICT has only recently become vital for organisations in Thailand, and now this new act is forcing organisations to comply with this law as a baseline, as noted by the RAD/CIO.

5.2.5 Organisational ICT strategy

The RAD/CIO mentioned that this organisation intends to improve ICT risk management and to mitigate ICT risk by focusing on four categories: governance, operations, development and compliance, which all relate to the COBIT and ITIL frameworks (Figure 5-9). The RAD/CIO further stated that the ISO/IEC 17799 standard is the main focus of its ICT security risk management, while the COBIT and the ITIL frameworks supplement the ICT risk management planning, as shown in diagram below.



1. Planning and Organising
2. Organisation of Information Security
3. Compliance
4. Human Resource Security
5. Physical and Environmental Security
6. Access Control
7. Delivery and Support
8. Monitoring
9. Information System Acquisition and Development
10. Business Continuity Management

Figure 5-9: ICT risk management goals and planning: Case study E

According to the RAD/CIO recommendations, this organisation uses the COBIT framework and the ITIL framework to manage organisational governance, operations,

development and compliance as ICT risk management planning to supplement ICT security risk management. From there, these four areas help the organisation to define information security policy by using the ISO/IEC 17799 standard.

5.2.6 Summary

The key factors addressed by, and which were the focus of, ICT risk management in this organisation were:

- policy;
- management of ICT resources;
- human resource management and planning or the management of people and their behaviour in the organisation;
- information security management; and
- ICT risk management planning.

Policy for ICT risk management is set as both global and local policy to provide organisational guidelines for staff to follow. In this regard, local policy is divided into ICT policy and Information security policy for dealing with ICT risk management. ICT and IS policies are a major focus because, as the interviewees explained, they are the two key areas which are imperative for dealing ICT risk management in this organisation.

ICT resource management is another success factor that this organisation uses to control ICT operation. ICT operation involves hardware, software and networks that penetrate the normal duties and functions of staff members. Therefore, this ICT operation is controlled in terms of providing appropriate and adequate ICT resources. Moreover, this organisation considers that ICT operation not only covers its own internal ICT processes but also relates to the service function for its clients.

Human resource management and planning is another key factor for this organisation in terms of controlling human error, and human resources protection and security. This factor is raised to control human risk and/or operational risk which can be difficult to control and protect. The setting of roles and responsibilities for staff members is part of this key factor in this organisation.

Information security management is a key factor to which this organisation pays attention because it helps control user management, user account management, user authority, user rights and security plans (i.e. personal firewall, filter spam and access

control). By doing so, this organisation can maintain its own systems using scanning tool software. Moreover, this organisation can also monitor any network port and only provide the network port for its own computers in order to mitigate, avoid and prevent any type of risk related to ICT.

Lastly, reflecting on these practices in relation to the research purposes, this organisation establishes ICT risk management at the corporate level, which equates to a top-down process. The corporate level plan is then communicated to the operations level to develop its own operational plan. Therefore, in this organisation the key factors for ICT risk management planning include policy; ICT resource management; IS management; and human resource management and planning, which all directly affect the corporate level plan and indirectly affect the operational level plan in maintaining successful ICT risk management.

5.3 Case study F

5.3.1 Organisational profile

This organisation delivers two types of business service—auditing and consulting—which cover a wide range of services. The risk management process is a critically important area of this organisation. The organisation assists firm clients to control and assess business risk by identifying and quantifying risk exposure and implementing systematic processes to manage risk. Their staff assist businesses to take advantage of opportunities derived from an improved understanding of risk, and ensure that management of risk is an explicit and integral part of everyday business. Its services regarding ICT risk management fall into the realms of corporate governance, risk management, internal audit, control assurance, application security, infrastructure security, information security management and business continuity planning.

5.3.2 Organisational structure

Roles and responsibilities

This organisation has a global audit committee which is responsible for business and ICT risk management within the organisation (Figure 5-10). The Senior Consultant explained that the audit committee is responsible for the core business processes. In contrast, the ICT risk management plan in this organisation is the responsibility of the risk management committee which allocates duties to staff in relation to dealing with ICT

risks. The risk management committee in this organisation is where the ICT risk management plan is developed and directed, as shown in Figure 5-10 below.

Figure 5-10: Roles and responsibilities: Case study F

The Senior Consultant explained:

> *"As we are an international consulting organisation, we need to follow the main office to conform to regulations and rules from the global audit committee. Focusing on ICT risk, the risk management committee is responsible for this."*

ICT risk management treatment

In terms of consultation, the Senior Consultant mentioned that his clients' organisations provide a framework for dealing with ICT risk for coordination at the corporate level. A framework based on organisational policy is best formulated at the corporate level (Figure 5-11). Such a framework will help an organisation to define an ICT risk management plan in order to prevent, avoid and mitigate ICT risks. In this regard, the Senior Consultant mentioned that defining the ICT risk management plan covers governance strategy, risk management policy and an action plan. Once the scope of the ICT risk management plan is established, his clients' organisations can establish their own methodology for dealing with ICT risks.

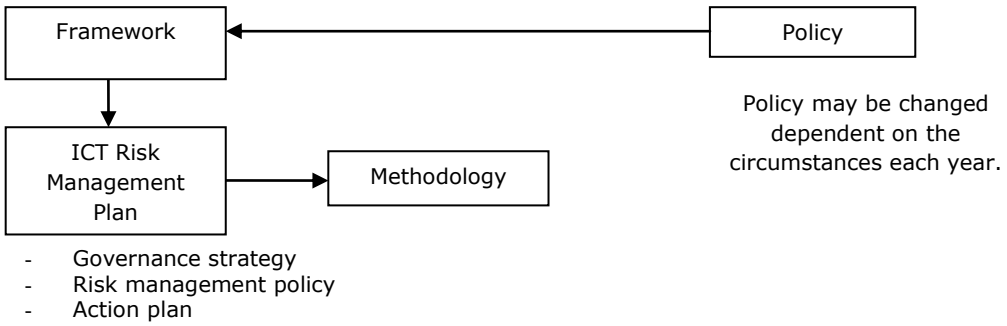


Figure 5-11: A framework for ICT risk management treatment: Case study F

Components of ICT risk management

According to the consultation perspective, the Senior Consultant noted that ICT control and audit in Thailand is still not well established because Thai organisations do not clearly separate the roles and responsibilities related to internal audit (business concern) and ICT audit (ICT concern) in his clients' organisations. Most Thai businesses, especially his clients, use an internal auditor as their ICT auditor, yet the Senior Consultant argued that this approach is not appropriate because it leads to a lack of sophistication and thus an inability to handle the complexity of ICT matters. Therefore, the Senior Consultant concluded that ICT control and audit must take into account information technology and information security.

5.3.3 Organisational process

ICT risk management instrument

In practice, the ICT risk management process in this organisation is identified by six processes that the organisation considers when dealing with ICT risks (Figure 5-12). These six processes are used to help the organisation to understand:

- what types of risk (identify and classify risks) the organisation encounters;
- the probability that a risk may occur, and its impact;
- what type of strategy needs to be provided to deal with risk;
- how the strategy provided is deployed;
- the effectiveness of ICT risk management; and
- what risk assessment program needs to be adopted and whether ICT risks are mitigated to an acceptable level.

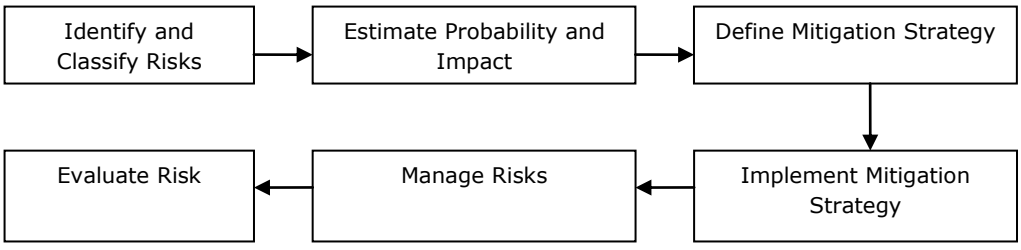


Figure 5-12: ICT risk management instrument: Case study F

The Senior Consultant described each of these steps in greater detail, explaining that risk identification entails a comprehensive identification and assessment of potential risks.

The potential risks include both internal and external risks. Internal risks relate to organisational strategy, operations and management programs, specifically how well these three areas are implemented in an organisation and which processes within them are poorly conducted.

Secondly, estimating the probability and impact of identified risk from the first step is undertaken to ensure that the potential risks from both the internal and external environment do not threaten business strategies, objectives and goals. However, if there is a high probability that these potential risks will occur, or if they are likely to be significant, then the next step is required.

Thirdly, defining the mitigation strategy is undertaken to address the core challenges of the risks and define the most effective and least costly or time-consuming ways to reduce both the impact and probability of the potential risks. By doing so, the organisation translates the core business transaction into business operations, training and services so that it can focus on only those areas threatened by a high risk impact and high risk probability. From there, the organisation can develop a mitigation strategy tailored to the risks in a specific area. Once the mitigation strategy is defined, it is taken to the next step.

Fourthly, the mitigation strategy is implemented which involves measuring how effective the strategy is for the specific area and who is responsible for the strategy. By doing this, this organisation can eliminate potential risks, ensure that risks are mitigated, accept where there is potential risk and manage those potential risks appropriately.

Fifthly, managing risk is used to evaluate the potential risk and the magnitude of ICT risk. The effectiveness of ICT risk management is revealed by how well it mitigates, avoid and prevent potential risk, so that it is maintained at an acceptable level. Lastly, evaluating risk is undertaken simultaneously with managing risk because the outcome of these two steps is to evaluate the potential probability and impact.

5.3.4 Organisational control

Human resources

This organisation regulates human resources through a three-stage process. Starting from the input process, all new staff must sign the employment agreement of this organisation that delineates their obligations in relation to compliance to the organisation’s guidelines on ICT risk. This aspect of the agreement is aimed at preventing the occurrence of ICT risks that result from misunderstandings about information

disclosure and confidentiality. This organisation thus ensures that all staff are trained and educated on these matters. The output process concerns the end of an employment contract or transferring an employee, requiring that the organisation remove the previous roles and responsibilities of an employee who resigns, and replace or change the relevant personal access codes or passwords, as outlined by the Senior Consultant.

Control process

In this organisation, the ICT risk management process is embedded in internal control and audit. Internal control and audit mainly focuses on enterprise risk management (ERM) which covers business risk and ICT risk management (Figure 5-13). The Senior Consultant described how, with regard to ICT, most control processes derive from the COBIT framework, which provides guidelines to senior management in this organisation. This organisation then uses this to plan its organisational strategy (the strategic components of ICT governance), operations (the operational components of ICT governance), and transformation (project change management and human resource management processes) in order to mitigate strategic risks, operational risks and financial risks respectively.

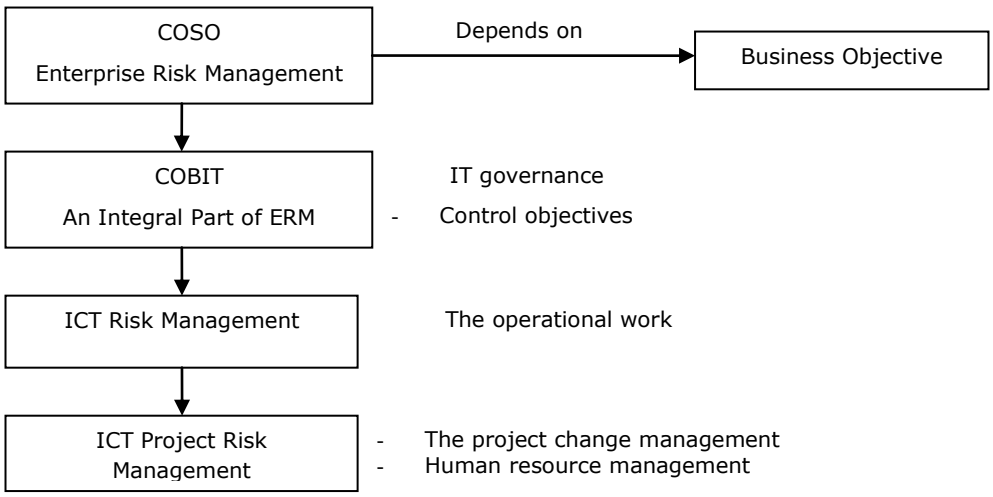


Figure 5-13: Control process: Case study F

Technology and systems

In terms of consultation, the Senior Consultant argued that clients' organisations separate technology and systems into two types of ICT and system control. The internal environment is the first area of ICT and system control which is defined by control of ICT application and information security, as explained by the Senior Consultant. He further outlined that ICT application is controlled by focusing on general ICT which is relevant to ICT management. In contrast, information security is controlled by focusing on information security policy including password updates, policy maintenance and system control. The second type of ICT and system control is relevant to the external environment, which is identified by outsource vendors (ICT outsourcing) regarding the

service level agreement (SLA) between a vendor and the client organisation, as noted by the Senior Consultant.

5.3.5 Organisational ICT strategy

The Senior Consultant revealed that organisational ICT strategy in this organisation is mainly focused on the COBIT framework to set the organisational strategy, operation and transformation (Figure 5-14). The ISO/IEC 17799 standard is supplementary, informing the technical aspects of this organisation's operations.

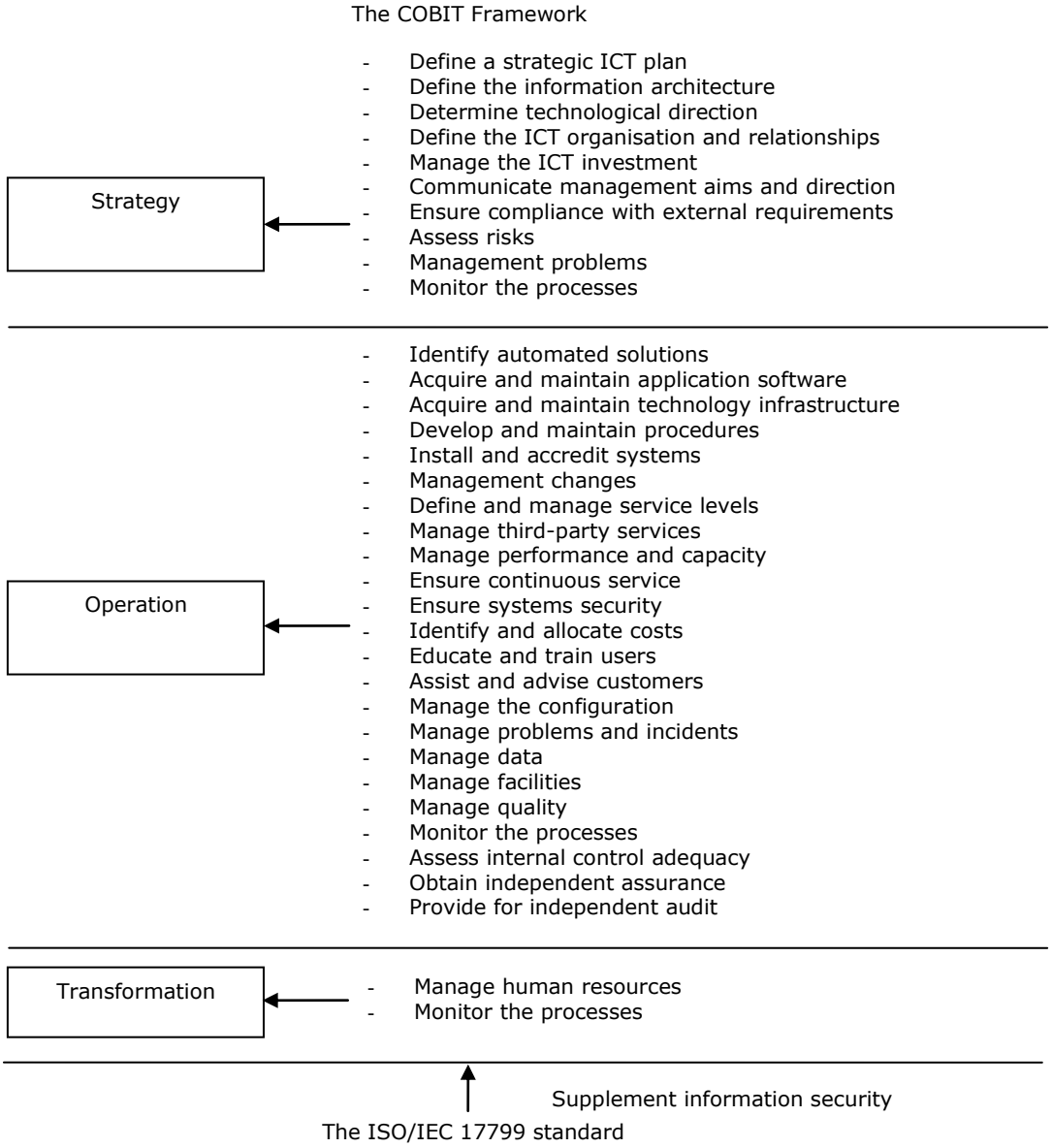


Figure 5-14: Control objectives for organisational ICT strategy: Case study F

The Senior Consultant added that the strategy in this organisation is generated from the COBIT framework by selecting from its control objectives, as shown in Figure 5-14. He

also explained the organisational operations are activities that his organisation pays more attention to undertake ICT process. The operational activities in this organisation are also controlled by using the control objectives from the COBIT framework, as shown in Figure 5-14. Next, the transformation is to help this organisation to rotate the roles and responsibilities of staff to perform in different duties in their department, and is used to manage and control the roles and responsibilities of human resources in this organisation. The transformation is drawn from the control objectives in the COBIT framework as shown in Figure 5-14. Lastly, information security management is used to supplement the security of all business transactions in this organisation by reference to the ISO/IEC 17799 standard, as represented in Figure 5-14.

5.3.6 Summary

The key factors addressed by, and which were the focus of, ICT risk management in this organisation were:

- policy:
- management of ICT resources;
- human resource management and planning or the management of people and their behaviour in the organisation;
- information security management; and
- ICT risk management planning.

Policy for ICT risk management is the first key factor that is used to guide the direction of this organisation. This factor covers business and ICT, including ICT and IS policies. According to the direction of the audit committee in this organisation, organisational strategy is divided to deal with ICT risk management in two directions (i.e. business and ICT). Therefore, business policy defines the business process, and ICT policy defines the ICT and IS process in this organisation.

ICT resource management is considered a key factor in this organisation. This factor is the focus for determining how ICT resources are managed and provided to staff members. This key factor relates to ICT application in this organisation

Another key factor in this organisation is information security management, which relates to system control including password updates, policy maintenance and information

security in ICT application. The main focus of this key factor lies with technical matters, specifically managing the complexity of ICT matters.

Human resource management and planning is a major concern in terms of the roles and responsibilities of staff members in this organisation. Human resource management and planning includes the protection of staff members through a three-stage process: employment agreement, during employment and termination of employment.

Lastly, aligning this organisational practice with the research purposes, ICT risk management is treated by the risk management committee where senior management develops and directs ICT risk management planning. This implies that this organisation performs and plans ICT risk management at the corporate level. The corporate level plan will then lead to the development of the operational level plan for dealing with ICT risk management. Moreover, organisational policy; ICT resource management; IS security; and human resource management and planning are critical factors in this organisation which are used to achieve successful ICT risk management, as revealed from the interviewees' accounts. Each success factor is explained in the following.

5.4 Conclusion

This chapter has presented a discussion of the current profile of ICT risk management in organisational practice for the case studies D, E and F. Based on the participants' views, ICT risk management is undertaken in relation to organisational structure, process, control and strategy. Each element of ICT risk management is discussed in turn next, with reference to the literature.

Organisational structure

Firstly, ICT risk management is governed by a separate committee which is responsible for different tasks in case studies E and F relating to ICT risk management. Case study D did not have a committee to take responsibility for the ICT risk. However, case study D described the roles and responsibilities related to ICT risk management in terms of the consultation experience of the interviewees, specifically referring to how the company's client organisations managed ICT risk. Case study organisation D determined that ICT risk management is the main responsibility of senior management, embedded in organisational strategy. Case study organisation E has a risk management partner to take responsibility for risk management, including business, ICT and IS risks. The risk management partner in case study E assigns the audit committee to take charge of risk management. The audit committee in this organisation directs and monitors all types of risk including business, ICT and IS, regardless of the technical sophistication or

knowledge of the internal auditors when dealing with ICT and IS risks. In contrast, case study organisation F has an audit committee and a risk management committee which are responsible for risk management. In relation to ICT risk, the risk management committee in this organisation pays particular attention to providing an ICT risk management plan for its staff to follow.

Secondly, the position level appropriate for ICT risk management treatment is considered important only by case study organisations D and F, but in each case from a different perspective. Based on their consulting experience, one of the interviewees from case study D suggested that ICT risk must be controlled and audited at both the corporate level and the operational level in order to help the organisation cover the treatment at both the origin of risk and at the risk impact. However, the other interviewee from case study D did not agree with this view, believing instead that ICT risk management should only be undertaken at the corporate level. In fact, organisation D provides ICT risk management treatment only at the corporate level. However, the operational level then follows the corporate plan when treating ICT risks. Similarly, case study organisation F also initiates ICT risk management treatment at the corporate level, for the operational level to follow.

Thirdly, the components of ICT risk management include ICT control and audit as well as information security control and audit. According to organisations D and E and F, ICT risk management relates to ICT activities and information security activities when dealing with ICT risk. All organisations have set the terms for ICT activities within ICT policy, and information security activities within Information security policy. This means that the staff understand their roles and responsibilities when facing any type of risk from ICT, and that they report such incidents to the board.

Organisational process

Firstly, the risk statement is seen from a different perspective according to the position level. However, the details in the risk statement cover the process for the both the entire organisation and for specific functions in the organisation. From the perspective of the interviewees from organisation D, the risk statement is viewed as an ICT risk management instrument for the staff to follow at both the corporate level and the operational level. With regards to the meaning of the risk statement at both levels, ICT risk management is used to clarify the risk methodology in corporate and operational plans. For example, in the corporate plan regarding ICT risk management, the organisation sets the overall scope of ICT risk management. Furthermore, in the operational plan, the organisation sets the details of ICT risk management processes in line with the corporate plan. This establishes a clear process statement for dealing with ICT risk in its client organisations. Conversely, organisations E and F mainly focus on

providing the overall process of ICT risk management to all staff levels in the organisation.

Secondly, in order to define the processes in the organisation, organisation F follows the guidelines from the internationally accepted framework of COBIT (ICT management), and the standard of ISO/IEC 17799 (information security management), as well as from enterprise risk management (business risk management) and ITIL (ICT services management). Case study organisation F is concerned with the appropriate processes from the COBIT framework, the ITIL framework and the ISO/IEC 17799 standard aligning with the ERM. These four standards can help organisation F to develop a methodology for business risk management, and ICT risk management including ICT resources, ICT services and information security. Case study organisation F mainly focuses on a top-down approach driven by the corporate level, thus communicating its policy direction to the operational level. On the other hand, organisations D and E follow the COBIT framework, the ITIL framework and the ISO/IEC 17799 standard in order to specify the appropriate processes for ICT management, ICT services and information security perspectives through a corporate-level top-down process, which is then transferred to the operational for delivery through a bottom-up process.

Organisational control

The common concerns across all case study organisations are over the control of people, process, technology and systems. Because they are similar consulting organisations, organisations D, E and F concentrate on the control of business, service, ICT and IS functions simultaneously. By doing so, human resource management is emphasised because organisations D, E and F believe that staff are the main trigger of ICT risk, whether intentionally or unintentionally. The delivery of training and education programs is a method used by all three organisations. Participants from all three companies believed that this method can help their organisation to raise awareness of human resources regarding the control of human risk or operational risk, which can be difficult to control and protect. Case study organisations D, E and F also believe that through education and training staff members can better understand the direction of control in terms of technology and security. In this regard, organisations D, E and F formulate their control objectives to direct organisational processes regarding business, services, technology and security processes. Case study organisation D participants explained that its control objectives are focused on a process of information systems management; a process of defining strategy; a process of security system; a process of systems development and change; and a process of business continuity management. In doing so, organisation F concluded that these control processes help mitigate strategic, operational and financial risks.

Organisational ICT strategy

Organisational ICT strategy as revealed through these three case studies illustrates that these organisations focus on ICT risk management in different ways. However, the interviews raised common issues and concerns in relation to ICT strategy. Furthermore, both top-down and bottom-up processes are considered valuable by similar types of business, which type of approach is best clarified when an organisation first begins planning around ICT risk management. Case study organisations E and F established risk management planning at the corporate level within the overall ICT plan, which then directs the operational plan by covering both ICT management and IS management. In contrast, a perspective revealed in case study D was that ICT risk management should be considered and planned at both the corporate and operational levels, as ICT risk management and ICT project risk management respectively. Moreover, different management levels (senior and operational managers) in the case study organisations were concerned that the ICT risk management plan might be divided between departments, meaning there is no consensus agreement at both levels. This means that ICT risk management is planned at the corporate level to cover the overall scope of ICT risk management, while the operational level plans ICT project risk management in detail within each relevant department. However, in this case both ICT risk management and ICT project risk management can be planned in the same direction according to the overall organisational ICT risk management plan. In this regard, it can be seen that successful ICT risk management planning focuses on collaboration between the management level activities and the operational level activities in order to deal with ICT risks effectively.

According to four themes, certain key factors emerged from the interviews which are seen to determine successful ICT risk management in each organisation. The key factors in case study organisations D, E and F are policy; management of ICT resources; human resource management and planning; information security management; the corporate level plan; and the operational level plan. In case studies D, E and F it was revealed that ICT risk management is focused at both the corporate and operational levels. The corporate level sets the overall ICT risk management plan, while the operational level establishes the specific technical security plan for ICT. Furthermore, for both the corporate and operational levels in the three organisations it was revealed that policy; human resource management and planning; information security management; and management of ICT resources are the key factors to consider when dealing with ICT risk management. The next chapter discusses the cross-case analysis (among case studies A, B, C, D, E and F) and the survey development based on the qualitative findings from Chapter 4 and this chapter.

Chapter 6
PHASE II: SURVEY DEVELOPMENT

This chapter reports on the cross-case analysis among all six case studies, and the survey development based on the key conclusions of Chapters 4 and 5. The key conclusions from Chapters 4 and 5 reveal that policy, human resource management and planning, management of ICT resources and organisational information security management affect both the corporate level and operational level plan when maintaining successful ICT risk management. This chapter begins with a comparative analysis of case studies A, B, C, D, E and F by comparing themes derived from Chapters 4 and 5. The cross-case analysis concludes the qualitative findings in comparison with the COBIT framework and the ISO/IEC 17799 standard. This chapter then develops indicators for each construct and constructs. The chapter concludes with an outline of the development of both the survey questionnaire and the conceptual model, which are validated in Chapter 7.

6.1 The cross-case analysis of the six case studies

Four different kinds of business (banking, telecommunications, software development and international consulting) are represented in the six case studies reported in Chapters 4 and 5. Each case study represents an exemplar of an effective way of dealing with ICT risk management. However, certain key points are highlighted, which demonstrate both similar and opposing perspectives. The common standards and frameworks, like the COBIT framework and the ISO/IEC 17799 standard, are used and recommended in the six cases for the control and management of ICT risk to an acceptable level. The key organisational elements for dealing with ICT risk management can be categorised into four main perspectives: organisational structure, organisational process, organisational control and organisational technical strategy.

On the basis of the case study findings, a thematic analysis of organisational elements related to ICT risk management was undertaken, out of which emerged the following:

1. Organisational perspective, which composed of:

   a. Roles and responsibilities, which were categorised according to:
      i. Audit committee (business process)
      ii. ICT committee (information and communication technology—ICT process)
      iii. IS committee (information security—IS process)
   b. ICT risk treatment, which was concerned at:
      i. The corporate level
      ii. The operational level
   c. Components of ICT risk management, which were classified by:
      i. ICT control and audit
      ii. IS control and audit
2. Organisational process, which was referred to:
   a. Instrument (risk statement), which was focused upon:
      i. ICT risk management methodology
      ii. ICT risk project management methodology
3. Organisational control, which was categorised by:
   a. People
   b. Process
   c. Technology and systems
4. Organisational Technological Strategy can be explained by either:
   a. a top-down approach, or
   b. a bottom-up approach
5. Other issues related to ICT risk management in organisations.

ICT risk management in the six case studies is embedded in the internal control and audit function. Internal control and audit in these organisations assume the main responsibility of risk management. All six organisations confirmed that their organisation reviews and defines its own internal control and audit policy to control both business risks and ICT risks. ICT governance has been shown in the COBIT framework to assist Thai organisations to provide strategic direction for technology in order to achieve business goals and objectives and to deal with ICT risks (ITGI 2007). ICT governance in the case studies has been focused on two main perspectives: ICT operations and ICT

security. ICT operations are managed at the corporate level in these organisations, and are defined clearly in the corporate plan in order to deal with ICT risk appropriately. ICT security is clarified at the operational level (the term 'the operational plan' and 'the action plan' are used interchangeably in this research), whose action plan or the operational plan is then provided to senior management for review and revision to ensure compliance across the entire organisation. The themes of the qualitative analysis arose from the case studies are discussed next.

6.1.1 Organisational perspective

Organisational structure was highlighted in the six case studies as requiring review before planning ICT risk management in these organisations (Table 6-1). The case study organisations were all concerned with the appropriate allocation of responsibility to employees with regard to risk management. This role allocation is initiated not only from the top to be delivered down, but also takes place at the bottom and is communicated to the upper levels in order to reach a consensus plan for the whole organisation. A consensus plan also provides the details of ICT risk components which must be assigned to roles of relevant staff in the organisation. A consensus plan covers the responsibilities of staff dealing with ICT risk; the roles and tasks involved in controlling ICT risks; ICT risk management procedures; and controlling the main components of ICT which the risks might threaten.

Table 6-1: A summary of the cross-case comparison of organisational perspective

Main process	Case A	Case B	Case C	Case D	Case E	Case F	Similarities	Differences	Findings
Define roles and responsibilities for ICT risk management	Define - Audit committee[1] - Risk management committee[2] - Enterprise-wide security committee[3]	Define - Audit committee	- Not specified	- Not specified	Define - Audit committee	Define - Global audit committee - Audit committee - Risk management committee	Define - Roles and responsibilities for business direction	Define - Roles and responsibilities for ICT and Security directions	Focus on roles and responsibilities of - Business - ICT - Security
Define ICT risk management treatment	Treat at - The corporate level - The operational level	Treat at - The corporate level - The operational level	Treat at - The project management which acts as the operational level	Treat at - The global level - The corporate level - The operational level	Treat at - The global level - The local level	Treat at - The global level - The local level • The corporate level • The operational level	Treat at - Top-down approach - Bottom-up approach	Treat at - The project approach	Focus on - Management view - Operational view - Project view
Define components of ICT risk management	Define - ICT resources - ICT security	Define - ICT resources - ICT security	Define - ICT security	Define - ICT resources - ICT security	Define - ICT resources - Information security (IS)	Define - ICT management - Information security	Define - ICT resources - Information security management	-	Concern with - ICT function - IS function
Define components of ICT control and audit as general IT	Define - ICT applications - Risk assessment	Define - Applications - Operating system - Networks - Other ICT systems	- Not specified	Define - ICT operation	Define - Hardware - Software - Networks	Define - ICT resources	Define - ICT resources	-	Associated with - Management of ICT resources
Define components of ICT security or security ICT	Define - ICT security in security policy	Develop - ICT security in security policy	Define - ICT security in project management	Define - ICT security	Define - ICT security management	Define - ICT security management	Define - Information security management	-	Associated with - Information security management
Define a risk statement	Define - A risk statement as an entire organisational plan	Define - A risk statement as an entire organisational plan	Define - A risk statement as a project management plan	Define - A risk statement as an entire organisational plan - A risk statement as a specified functional plan	Define - A risk statement as an entire organisational plan	Defined - A risk statement as an entire organisational plan	Define - A risk statement as an entire organisational plan	Define - A risk statement as a specific plan (project management)	Declare a risk statement at - The corporate level - The operational level as a project

1. Audit committee is in charge of business risk.

2. Risk management committee is in charge of all types of risk.

3. Enterprise-wide security committee is in charge of ICT security risk in particular.

Firstly, in all of these case studies setting up a committee determines those responsible for directly controlling a particular area of ICT risk management. This classifies the tasks for dealing with ICT risk into three areas: business direction, technological direction and security direction. Each direction is supported by the Board of Directors or the management committee. These approaches help the organisations to define responsibility for specific matters in particular areas, in turn to achieve business goals and objectives. Moreover, these approaches help organisations to define business and ICT processes, and organisational relationships. For example, case study organisation A divides the main tasks of the management committee into three areas in order for each objective to be managed separately. This illustrates that business objectives, ICT objectives and security objectives are taken into account at the same time that this business is growing. Moreover, each committee has the ability to define its own processes and to understand the circumstances surrounding the business in order to achieve the organisation's goals and objectives.

In terms of a systematic plan, it can be seen that these case studies reveal well-defined business processes, ICT processes, organisational relationships and management of information security. This reflects the usage of the control objectives of the COBIT framework and the ISO/IEC 17799 standard in planning, organising and management of information security.

Secondly, ICT risk management treatment is a focus at both the corporate and the operational levels. Each level is responsible for different tasks related to defining the business direction, technological direction and information security direction. The corporate level determines the corporate plan in respect to ICT risk management as an entire organisational plan. In contrast, the operational level must determine the action plan with specific technical details to serve the corporate plan of the organisation. After development, the action plan is then fed back to the corporate level for review, to ensure it fits the business, technology and technical criteria for a particular function.

Both the top-down approach and the bottom-up approach are implemented as part of a consensus agreement on how to deal with ICT risk management. The COBIT framework is used at the corporate level to set the corporate plan for dealing with ICT risk management as an entire organisational plan, as evidenced in all case studies. This falls within the domain of planning and organising around determining technological direction and managing projects. Conversely, the ISO/IEC 17799 standard is used at the operational level to set the specific action plan for dealing with ICT risk management. It is mapped with security policy and the management of information security.

Thirdly, ICT risk management includes the components general ICT control and audit, and ICT security control and audit. General ICT control and audit must ensure that all

general ICT matters are controlled and audited properly by focusing on ICT risk management methodology. In essence, in all of the case studies except for case study C management utilises the COBIT framework to align ICT strategy with business strategy. Case study C, conversely, is concerned only with the information security component rather than ICT management because this organisation deals in software development. The major tasks of software development involve computer programming; as a result the process of ICT risk management focuses only on the technical perspective. However, most case study organisations were of the opinion that the COBIT framework should be used to set the overall ICT strategy as part of the overall organisational plan. On the other hand, the ISO/IEC 17799 framework is used to set the specific technical details on information security, as shown in case study C. It is mapped with the operational level rather than the corporate level. In order to effectively plan ICT risk management, these organisations consider using both the COBIT framework and the ISO/IEC 17799 standard to generate specific plans at different levels. In this regard, the COBIT framework and the ISO/IEC 17799 standard supplement each other in ICT risk management planning, as shown by case studies A, B, D, E and F.

Fourthly, in regard to ICT control and audit (i.e. general ICT), it has been illustrated in these case studies that people, process, technology and systems are controlled and monitored by focusing on ICT applications, operating systems, networks and other ICT systems (i.e. ICT management). Thus, it is important that general ICT is managed properly. People, process, technology and systems are represented in the COBIT framework in the control objectives of information architecture, technology resources and information technology process. Moreover, the COBIT framework stipulates that these four processes be monitored in the planning and organising domain.

Fifthly, it has been shown that, as a component of ICT security control and audit (i.e. ICT security), all types of information security techniques are performed in association with the security transaction embedded in business and ICT processes. It is evident that the six case study organisations pay more attention to security policy in dealing with ICT security risk by using the information security management standard of the ISO/IEC 17799 standard. On the other hand, the COBIT framework does not clearly specify ICT security techniques because it is a framework for setting ICT governance at the highest level, according to the interviewees. Thus, ICT security control and audit follow the standard of information security management (i.e. the ISO/IEC 17799 standard) by focusing on security management.

Lastly, a risk statement is used in these organisations to define ICT risk methodology. The methodology of the risk statement provides a brief outline of ICT risk management as an overall plan. From there, this plan is transferred to the operational level to be

applied to a specific technical area in order to fit with a particular function. This risk statement is provided by both the corporate level and the operational level. However, a risk statement at the corporate level is a vital part of an operational risk statement because it is relevant to a corporate risk statement. It is discussed next.

6.1.2 Organisational process

The ICT risk management instrument is vital for determining the ICT risk management process at both the corporate and operational levels (Table 6-2). Moreover, an ICT risk management instrument serves an entire organisation as an overall plan in association with business objectives, technological objectives and technical security objective. In this regard, the case study organisations separate their ICT risk management instruments into one at the corporate level and one at the operational level. Nevertheless, the corporate risk management instrument provides an overall ICT risk management processes, in contrast, the operational risk management instrument further details technical matter regarding information security systems. Both of these then instruments supplement each other to help their organisations follow a common direction. Moreover, the ICT risk management instrument is outlined by the COBIT framework in planning and organising domain, and by the ISO/IEC 17799 in the area of communication and operation management.

A risk statement is an example of an ICT risk management instrument which the six case study ICT risk management used to explain the main roles of ICT risk management at both the corporate level and the operational level. A risk statement outlines the responsibilities entailed in risk management, risk management methodology, risk control and auditable areas. A risk statement is used to determine the responsibilities of management and operational staff in regard to directing, operating, monitoring and treating risk. The methodology of a risk statement is explained in the setting of risk objectives, risk identification, risk assessment, risk response and risk monitoring as presented in the COBIT framework and the ISO/IEC 17799 standard. Risk management methodology is performed by management and operational staff simultaneously. Mapping with the COBIT framework and the ISO/IEC 17799 standard, the control of the risk statement and its auditable areas is presented in the section on assessing and managing ICT risks and managing projects in the COBIT framework. In contrast, the risk statement and its auditable areas are covered in the section on communications and operations management in the ISO/IEC 17799 standard.

Table 6-2: A summary of the cross-case comparison of organisational process

Main process	Case A	Case B	Case C	Case D	Case E	Case F	Similarities	Differences	Finding
Define ICT risk management instrument	Define - ICT risk instrument at the senior management level	Define - ICT risk instrument at the senior management level	Define - ICT risk instrument at the operational level	Define - ICT risk instrument at the senior management level - ICT risk instrument at the operational level	Define - ICT risk instrument at the senior management level	Define - ICT risk instrument at the senior management level	ICT risk instrument is defined at the senior management level	ICT risk instrument is defined at the operational level	Provide ICT risk instrument for both - The corporate function - The operational function
Define A risk statement as instrument	Define the statement of ICT risk methodology in - The corporate level plan	Define the statement of ICT risk methodology in - The corporate level plan	Define the statement of ICT risk methodology at - The operational as a project risk management plan	Define the statement of ICT risk methodology in - The corporate level plan - The operational level plan as a function	Define the statement of ICT risk methodology in - The corporate level plan	Define the statement of ICT risk methodology in - The corporate level plan	Risk statement is defined as the ICT risk methodology in the corporate level plan	Risk statement is defined as the ICT risk methodology in the operational level plan	ICT risk management methodology is defined in the corporate level and the operational level plans.
Define ICT risk management process	Implement - COBIT - ISO/IEC 17799	Implement - ERM - COBIT	Implement - ISO/IEC 17799	Implement - COBIT - ISO/IEC 17799	Implement - COBIT - ISO/IEC 17799 - ITIL	Implement - ERM - COBIT - ISO/IEC 17799	Implement - COBIT	Implement - ERM - ISO/IEC 17799 - ITIL	Clarify details of ICT risk management process in terms of - ICT risk assessment and management - ICT risk project assessment and management

The next section discusses the analysis of another theme which is organisational control.

6.1.3 Organisational control

Organisational control is divided into the areas of human resources, process, technology, and systems in the case study organisations (Table 6-3). The control of human resources is focused on human resources protection and security simultaneously because employees influence organisational management regarding business, ICT, security and service functions. Business function is controlled by directing the awareness of employees in relation to ICT in turn to avoid any obstacles to the business objectives. ICT function relates to employees in terms of the control of computer abuse such as sharing confidential data, files or databases. Security function is concerned with whether employees access, perform and treat digital data, files and information appropriately. In this regard, the COBIT framework and the ISO/IEC 17799 standard are used to manage such issues by focusing on the control objectives of managing IT human resources; educating and training users; access control; and human resources protection and security.

The control process focuses on the 'input', 'processing' and 'output' (IPO) processes of technological activities in order to monitor data through organisational processes (e.g. starting from generating data to disseminating information processes). It is imperative that the control process defines procedures that serve the business, ICT, security and service functions correctly and accurately. Thus, these four main functions must be served by proper procedures that define, manage and ensure the effectiveness of the business strategy, the ICT strategy and the security strategy.

Business function is relevant to employee performance in terms of providing the service function by using the ICT function and the ICT security function correctly and accurately. The case study organisations all define and manage business process to ensure it meets business objectives. Furthermore, defining business function is conducted not only at the corporate level but also at the operational level. At the corporate level these organisations provide the control objectives for managing problems, managing the physical environment and managing operations based on the COBIT framework. Whereas at the operational level these organisations provide the control objectives for information security incident management based on the ISO/IEC 17799 standard.

Table 6-3: A summary of the cross-case comparison of organisational control

Main process	Case A	Case B	Case C	Case D	Case E	Case F	Similarities	Differences	Finding
Control Human resources	Plan to control - ICT security awareness - Computer abuses - Educating and training program - Rules and regulations - Human resources security	Plan to control - Access control - Roles and responsibilities	Plan to control - Human resources protection and security	Plan to control - Information privacy - ICT security awareness - Educating and training program	Plan to control - ICT awareness - Agreement of information security policy	Plan to control - The employment agreement prior to employment, during employment and ending employment or transferring position	Plan to control - ICT and security awareness - Human resources protection and security	Plan to control - Roles and responsibilities as outlined in the employment agreement - Educating and training program - Rules and regulations as compliance	Plan to control - Business impact - ICT impact - Security impact
Control Process	Control the process of - Internal control - Information management - Security treatment - Setting the configuration - Penetration test - Security scanning tool - Auditable area	Control the process of - Internal control - Information management - Auditable area - Security management - Setting the configuration - Data authentication	Control the process of - Security in software development as project management	Control the process of - Organisation of information systems - Security systems - System development and changes - Business continuity management	Control the process of - Risk management software - Risk assessment in balance security score card	Control the process of - Internal control - Information management - Information security management	Control the process of - Information security management ○ Setting the configuration ○ Data authentication ○ Security scanning tool ○ Penetration test ○ Business continuity management	Control the process of - Internal control[1] ○ Auditable area - ICT management ○ Organisation of information systems ○ System development and changes ○ Business continuity management	Plan to control - Business process - ICT process - Security process
Control Technology and systems	Plan to control - ICT application - ICT security	Plan to control - General control - Application control	Plan to control - Communication infrastructure[2]	Plan to control - Data - Information	Plan to control - ICT application - ICT security	Plan to control - ICT application - Information security	Plan to control - ICT management - ICT security management	Plan to control - Service management	Plan to control - Service function - ICT function - Security function

1. Internal control is a major task of business process.

2. Communication infrastructure is controlled to provide the quality of organisational services for customers.

Service function is connected to internal and external services such that the case study organisations define and manage service process to ensure it meets service objectives. Service function is focused on defining and managing service levels; ensuring continuous service; and managing the service desk and incidents, as outlined in the COBIT framework. It is also focused on maintaining business continuity management based on the ISO/IEC 17799 standard, in order to achieve the competitiveness of business service in a timely manner in both internal and external operations. However, service function, including both the involvement of internal and external parties, remains unaddressed in this study. Furthermore, it is not mentioned in detail at this level because it relates to another standard of ICT service management called the Information Technology Infrastructure Library (ITIL).

ICT function also needs to be controlled to meet ICT objectives. The case study organisations all define and manage ICT function to ensure that it meets ICT objectives. ICT function penetrates not only the corporate level regarding managing performance and capacity, managing the configuration and managing data based on the COBIT framework, but also the operational level in connection to data and information integrity management based on the ISO/IEC 17799 standard.

It is necessary that security function also be controlled. These organisations all define and manage the security function process to ensure that it meets information security objectives. Security function not only penetrates the corporate level to ensure system security based on the COBIT framework, but also the operational level to provide physical and environment security and information security incident management based on the ISO/IEC 17799 standard.

Technology and systems are controlled by concentrating on ICT function at the corporate level and information security function at the operational level. ICT function is general ICT which includes overall ICT planning for matters such as networking, data management and infrastructure. ICT function is controlled by managing performance and capacity; managing the configuration; managing problems; managing data; managing operations; monitoring and evaluating IT performance; monitoring and evaluating internal control; ensuring compliance with external requirements; and providing ICT governance, as illustrated in the COBIT framework. Concurrently, ICT security is a specific technical area that requires management at both the corporate level, by ensuring systems security based on the COBIT framework, and the operational level, regarding communications and operations, and compliance based on the ISO/IEC 17799 standard.

The next section discusses the analysis of the last theme which is organisational ICT strategy.

6.1.4 Organisational ICT strategy

Organisational technical strategy mainly focuses on ICT strategy regarding ICT risk management planning and the revision of ICT departmental structure, as communicated by the interviewees (Table 6-4). ICT strategy is generally based on a top-down approach, which is similar to the direction stipulated in the COBIT framework. The COBIT framework asserts that overall ICT strategy planning is based at the highest level (i.e. senior management or the Board of Directors). Overall ICT strategy is then delivered to operational staff for implementation. Adopting this one-way approach (i.e. top-down approach) controls only one perspective; for example, the overall ICT plan is generated from the managerial perspective which leads to a singular focus on general ICT. Conversely, ICT security is not treated in this way. Thus, the interviewees revealed that a bottom-up approach as stipulated by the ISO/IEC 17799 standard can be used to develop organisational technical strategy by focusing on two directions when dealing with ICT risk management.

Generally, the COBIT framework is used to generate an ICT risk management plan at the management level in the case study organisations. It could therefore be claimed that ICT risk management planning is primarily influenced by management perceptions. Moreover, from the interviewees' perspectives the COBIT framework itself encourages management to plan ICT risk management as an overall ICT strategy without reference to specific technical areas. This approach is not able to deal with general ICT risks and specific ICT security risks simultaneously. Therefore, the operational level becomes vital to enrich the perceptions of ICT risk management by focusing on multiple perspectives regarding general IT and specific ICT security. It is therefore suggested, by the participants, that both the corporate and the operational levels plan ICT risk management together by reaching a consensus agreement on the plan. Lastly, the ICT department needs to review organisational structure in terms of managing the different roles and responsibilities related to general ICT function and ICT security function. However, general ICT function and ICT security function must be managed through a collaborative process. Thus, the question has been raised around why general ICT and ICT security functions are performed in different departments or areas. In fact, each function has its own roles and responsibilities for developing ICT risk management planning, yet organisation C still has only one department that is responsible for the two tasks (i.e. ICT management and ICT security). Therefore, this issue arose in the interviews with organisation C, and requires further consideration.

Table 6-4: A summary of the cross-case comparison of organisational ICT strategy

Main process	Case A	Case B	Case C	Case D	Case E	Case F	Similarities	Differences	Finding
Define Strategies	Defined from - The managerial perspective	Defined from - The operational perspective	Defined from - The operational perspective	Defined from - The managerial perspective - The operational perspective	Defined from - The managerial perspective - The operational perspective	Defined from - The managerial perspective - The operational perspective	Strategies are defined from the managerial perspective	Strategies are defined from the operational level perspective	Define organisational strategies as - Overall IT plan - Specific IT security details
Define ICT risk management plan	Include the plan in - The corporate plan - The operational plan	Include the plan in - The corporate plan - The operational plan	Include the plan in - The operational plan	Include the plan in - The corporate plan - The operational plan	Include the plan in - The corporate plan - The operational plan	Include the plan in - The corporate plan - The operational plan	ICT risk management plan is clarified in both the corporate plan and the operational plan	-	Define the plan as - Consensus plan at the corporate plan - Individual plan at the operational plan
Recommend Revision of IT department structure	- Not specified	- Not specified	- IT department - IT security function	- Not specified	- Not specified	- Not specified	-	Recommend to revise the role and responsibility of ICT function and ICT security function	Concern with - Direction of reporting to management

From the analysis of the comparison tables above and from the literature review in Chapter 2, the 14 key processes have been illustrated in relation to organisational structure, organisational control, organisational process and organisational technical strategy. Each key processes leads to different findings which represent the various perceptions of successful ICT risk management revealed in the case studies. The 14 key processes consisted of:

- defining role and responsibility for ICT risk management,
- defining ICT risk management treatment,
- defining components of ICT risk management,
- defining components of ICT control and audit as general ICT,
- defining components of ICT security or security ICT,
- defining a document of policy (i.e. a risk statement),
- defining ICT risk management instrument,
- defining ICT risk management process,
- controlling human resources,
- controlling ICT processes,
- controlling technology and systems,
- defining organisational ICT strategy,
- defining ICT risk management at the corporate level (i.e. a corporate plan),
- defining ICT risk management at the operational level (i.e. a operational plan), and

The 14 key processes embedded in the four themes (organisational structure, organisational control, organisational process and organisational technical strategy) are compared with the control objectives in the COBIT framework and the ISO/IEC 17799 before developing the survey in detail in the next section. The 14 key processes in the perception of the respondents in the case studies (reported in Chapter 4, 5 and this chapter) highlighted separate and sometime overlapping key factors as follows:

- defining organisational ICT strategy and defining a document of policy reflected the setting of policy in the case studies,

- defining components of ICT risk management, controlling ICT processes, defining components of both ICT control and audit reflected the management of ICT resources,

- defining components of ICT risk management, defining components of ICT security or security and controlling technology and system ICT reflected the management of information security,

- defining role and responsibility for ICT risk management and controlling human resources reflected the management of people and their behaviour in the case studies,

- defining ICT risk management treatment, defining components of ICT control and audit as general ICT and defining ICT risk management process at the corporate level reflected the planning of a corporate plan, and

- defining ICT risk management treatment, defining components of ICT security or security ICT and defining ICT risk management process at the operational level reflected the planning of an operational plan.

These processes then encapsulated the six key factors (policy, the management of ICT resources, the management of information security, the management of human resources, a corporate plan and an operational plan) that were discussed along with the comparison of the COBIT framework and the ISO/IEC 17799 standard. The foci of the six key factors are relevant to the COBIT framework and the ISO/IEC 17799 standard as outlined in the following section.

6.2 Comparing practices with the COBIT framework and the ISO/IEC 17799 standard

Six key factors (policy, the management of ICT resources, the management of information security, the management of human resources, a corporate plan and an operational plan) have been highlighted and recommended in the case studies. Each key factor can then be mapped with the COBIT framework and the ISO/IEC 17799 standard in order to reconfirm or reject them in the survey. The researcher used the control objectives from both the COBIT framework and the ISO/IEC 17799 standard to compare with ICT risk management practices in Thai organisations in order to develop the survey questions. Although the COBIT framework and the ISO/IEC 17799 standard cover different areas, this recommendation can help the researcher to explore success factor for the planning of ICT risk management by including policy, ICT applications (i.e.

technology management), ICT security (i.e. information security management) and employees and their behaviour in an organisation (i.e. human resource management and planning) and aligning the corporate plan with the operational plan. When considering both the corporate and operational plans, ICT governance context can help the researcher understand the direction of ICT risk management which can be referred to as:

> 'The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly' (ITGI 2006b, p. 11).

This recommendation also assists with the contextualisation of ICT risk management practice in Thai organisations as discussed in the remainder of this chapter. The control objectives are discussed in the following section based on the key factors identified from the case studies. The key factors and the relationship among them derived from the case studies were placed in the Successful ICT Risk Management (SICTRM), which has been followed by the researcher throughout this study.

6.2.1 Policy

Organisational policy can be defined based upon the control objectives of the COBIT framework, and the ISO/IEC 17799 standard which:

> 'provides strategic direction, ensures that objectives are achieved, [and] manages risks appropriately' (ITGI 2006b, p. 18).

This research identifies the necessary control objectives of policy to capture success factor of the SICTRM model.

The COBIT framework consists of:

- Defining a strategic ICT plan (PO1)[4]
- Determining technological direction (PO3)
- Ensuring continuous service (DS4)

The ISO/IEC 17799 standard consists of:

- Security policy

[4] From this point, the codes in the brackets are referred to as the control objectives in the COBIT framework.

- Organisation of information security
- Communication and operations management
- Business continuity management

In relation to organisational policy, both the COBIT framework and the ISO/IEC 17799 standard were considered when determining the control objectives above. The next section identifies important control objective concerning the management of ICT resources.

6.2.2 Management of ICT resources

ICT resource management can be defined based on the control objectives of the COBIT framework and the ISO/IEC 17799 standard. This area is aimed at:

> 'verifying that the enterprise's resources are used responsibly' (ITGI 2006b, p. 11).

This research outlines the control objectives required of management ICT resources to capture success factor of the SICTRM model.

In this regard, the COBIT framework includes:

- Procuring ICT resources (AI5)

In terms of the management of ICT resources, the COBIT framework is referred to in identifying the control objective above. The next section identifies important control objectives related to the HR management and planning to successful ICT risk management in Thai organisations.

6.2.3 Human resource management and planning, information security management, the corporate level plan and the operational level plan

Human resource management and planning, information security management, the corporate level and the operational level plans can be defined based on the control objectives outlined in the COBIT framework and the ISO/IEC 17799 standard. This focus of this area is as follows:

> 'Information security addresses the protection of information confidentiality, availability and integrity throughout the life cycle of the information and its use within the organization' (ITGI 2006b, p. 15).

This research stipulates the necessary control objectives of human resource management and planning, information security management, the corporate level and the operational level plans to capture success factor of the SICTRM model.

The COBIT framework consists of:

- Defining the information architecture (PO2)
- Defining ICT organisation and relationships (PO4)
- Managing human resources (PO7)
- Managing performance and capacity (DS3)
- Ensuring systems security (DS5)
- Educating and training users (DS7)
- Managing the configuration (DS9)
- Managing problems (DS10)
- Managing data (DS11)
- Managing the physical environment (DS12)
- Managing operations (DS13)
- Monitoring and evaluating ICT performance (ME1)
- Monitoring and evaluating internal control (ME2)

The ISO/IEC 17799 standard consists of:

- Organisation of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information security acquisition, development and maintenance
- Information security incident management
- Compliance

Both the COBIT framework and the ISO/IEC 17799 standard were referred to when identifying the control objectives above. The Thai business organisations consider ICT risk management by covering the four major areas of organisational policy; management of ICT resources; information security management; and human resource management and planning. These four major areas affect the planning at both the corporate level and

the operational level when seeking to establish successful ICT risk management. The next section discusses the comparison of ICT risk management practices from the case studies with literature, the COBIT framework and the ISO/IEC 17799 standard to develop the survey questionnaire.

6.3 Instrument development

Based on the findings of the qualitative analysis of the four sections in a theme (organisational structure, organisational process, organisational control and organisational technical strategy), the six key factors (policy, the management of ICT resources, the management of information security, the management of human resources, a corporate plan and an operational plan) derived from ICT risk management practices in the case studies. These six key factors are also the concern in the control processes of the COBIT framework and the ISO/IEC 17799 standard. The researcher then compared the practices with the control processes in both the framework and the standard to identify the items which indicate each key factor. Each key factor then was conceptualized in the model in order to reconfirm or reject to represent success factor for ICT risk management. Each key factor is discussed in greater detail below.

6.3.1 Dimension one: Organisational policy (POLICY)

Based on the analysis of participants in the case studies, it was recommended that organisations established a committee that is responsible for:

- ICT risk management (ICT and IS);
- ICT risk management instruments (a document of organisational policy);
- components of ICT risk management (consisting of ICT control and audit, and ICT security control and audit); and
- organisational ICT strategies (organisational policy).

Such a committee sets strategic direction, 'ensures that objectives are achieved, [and] manages risks appropriately' (ITGI 2006b, p. 18). Strategic direction on risk is often developed from the principles embedded in either the COBIT framework or the ISO/IEC 17799 standard, or both, because 'an organisation needs to define a strategic ICT plan and to determine technological direction and Information security policy in order to satisfy the business requirement and make possible the business strategy' (ITGI/OGC 2005, p. 23). Moreover, the document of organisational policy was referred in the case

studies to the risk statement that is a brief explanation of policy, of risk definition, of type of risk focused in the organization and risk management methodology. The document of organisational policy and business continuity management were also recommended, as confirmed by the interviewees, to determine technological direction and ensure continuous service of the COBIT framework and security policy of the ISO/IEC 17799 standard (Broderick 2006; ISO/IEC 2005; ITGI/OGC 2005, 2008; ITGI 2006a, 2006b and 2007). IT policy, Information security policy, a document of organizational policy and business continuity management reflected that the case studies considered organisational policy to be a key factor when dealing with ICT risk management, a view that is supported by Broderick (2006), ITGI (2006b), Karabacak and Sogukpinar (2006), McEvoy and Whitcombe (2002), Solms (2001), and Westby and Allen (2007).

The COBIT framework and the ISO/IEC 17799 standard were used to help the researcher define the indicators for organisational policy factor. Four main indicators were found to represent this key factor. Firstly, ICT policy was considered to evaluate how an organisation defines its ICT objectives around ICT direction when dealing with ICT risk management. Secondly, security policy was looked at to assess the way in which an organisation defines its IS objectives around information security when dealing with ICT risk management. Thirdly, the risk statement was included to evaluate how an organisation declares a statement of risk management in its corporate plan when dealing with ICT risk management. Lastly, business continuity management was examined to assess whether an organisation includes a brief explanation of continuous business management in its organisational policy when dealing with ICT risk management.

ICT policy, security policy, risk statements and business continuity management all enabled an organisation to plan at both the corporate level and the operational level to establish the conditions for successful ICT risk management (Table 6-5); and as such they were included in the summary to test the factors that affect ICT risk management in organisations.

Table 6-5: Policy dimension

Proposed dimension based on the qualitative analysis	Indicator	Main concern in the COBIT framework and the ISO/IEC 17799 standard
POLICY - IT policy (Q7) - Security policy (Q8) - Risk statement (Q9) - Business continuity management (Q10)	- policy1 - policy2 - policy3 - policy4	- Define a strategic ICT plan - Determine technological direction - Define information security policy - Define business continuity plan

Policy dimension referred to questions no. 7–10 in the questionnaire, listed below:

Q7. The organisation defines technological direction in the organisational policy.

Q8. The organisation defines security direction in the organisational policy.

Q9. The organisation establishes the risk context to define a brief explanation of ICT risks, of types of risk in the organisation and of risk management methodology.

Q10. The organisation has a business continuity plan to deal with the uncertain circumstances around the loss of information assets.

6.3.2 Dimension two: Human resource management and planning (HRMP)

Organisational control of people and their behavior in organisations was one of the key factors that arose from the case studies, one which organisations needed to take into account when planning ICT risk management. From the qualitative analysis, ICT risk from internal processes originates mainly with an insider, a finding that is supported by Ciborra (2006), Hermanson et al. (2000), Pinder (2006), Smith and McKeen (2006), Theoharidou et al. (2005), and Willcock and Griffiths (1994).

To gather rich information regarding human resource management and planning, the COBIT framework and the ISO/IEC 17799 standard were commonly recommended because both standards define the details of control objectives regarding human resource management and planning. Managing human resources; educating and training users; and monitoring and evaluating ICT performance using the COBIT framework were aimed at contributing to the indicators for human resource management and planning dimension (Broderick 2006; ITGI/OGC 2005, 2008; ITGI 2006b, 2007). Furthermore, human resources security as delineated in the ISO/IEC 17799 standard was also considered to highlight the indicators for the security of human resources (Broderick 2006; ISO/IEC 2005; ITGI/OGC 2005, 2008). Adopting the four control objectives (managing human resources; educating and training users; monitoring and evaluating ICT performance; and human resources security) of both standards, paying attention to the human resource management and planning factor can help an organisation to achieve effective control of human resources in order to mitigate, prevent and avoid ICT risks occurring from human error or ICT abuses (ITGI 2007; ISO/IEC 2005). Thus, it was essential that an organisation considered human resource management and planning derived from the the case studies when dealing with ICT risk management. A focus on human resource management planning was supported by Ciborra (2006), Hermanson et al. (2000), Pinder (2006), Smith and McKeen (2006), Theoharidou et al. (2005), and Willcock and Griffiths (1994).

To elaborate on human resource management and planning factor, both standards were used to define four indicators. Firstly, roles and responsibilities were examined to assess how an organisation manages human resources (referred to in the 'prior to employment' section in the ISO/IEC 17799 standard) when dealing with ICT risk management. Secondly, human resources protection was considered to evaluate whether an organisation includes terms and conditions of employment regarding confidentiality of information and disclosure of the organisation's important information (referred to in the 'prior to employment' section in the ISO/IEC 17799 standard) with the aim of dealing with ICT risk management planning. Thirdly, training and education was included to evaluate to what extent an organisation provides ICT and ICT security awareness training to its staff (referred to in the 'during employment' section in the ISO/IEC 17799 standard) when dealing with ICT risk management planning. Lastly, human resources security was looked at to evaluate how an organisation manages changing or removing the access rights of employees upon change or termination of employment (referred to in the 'termination or change of employment' section in the ISO/IEC 17799 standard) when dealing with ICT risk management.

Roles and responsibilities; human resources protection; training and education; and human resources security all helped an organisation at both the corporate and operational levels to plan and establish successful ICT risk management (Table 6-6); and as such they were included in the summary to test the factors that affect ICT risk management in organisations.

Table 6-6: Human resource management and planning dimension

Proposed dimension based on the qualitative analysis	Indicator	Main concern in the COBIT framework and the ISO/IEC 17799 standard
HRMP		
- Roles and responsibilities (Q13-Q16)	- hrmp1	- Organisational control of people
- Human resources protection (Q17-Q18)	- hrmp2	- HR access control and protection
- Training and education (Q19-Q20)	- hrmp3	- Educating and training users
- Human resources security (Q21-Q22)	- hrmp4	- Human resources security

Human resource management and planning dimension referred to questions no. 13–22 in the questionnaire, listed as follows:

Q13. The organisation defines employees' roles regarding information governance policy.

Q14. The organisation defines employees' responsibilities regarding information governance policy.

Q15. The organisation defines employees' roles regarding information security governance policy.

Q16. The organisation defines employees' responsibilities regarding information security governance policy.

Q17. The organisation declares the terms and conditions of employment regarding confidentiality of information.

Q18. The organisation informs employees that they must not disclose the organisation's important information.

Q19. The organisation provides a training program to improve staff's IT awareness.

Q20. The organisation provides a training program to improve staff's IT security awareness.

Q21. The organisation changes the access rights of employees upon change of employment.

Q22. The organisation removes the access rights of employees upon termination of employment.

6.3.3 Dimension three: Organisational information security (OS)

Organisational control processes (system configuration; access control policy; data and information integrity management; security compliance; and data protection and privacy) as discussed in the case studies emerged as organisational information security factor in this research. For example, case study C highlighted that organisational control processes constitute a technical matter related to organisational security that needs to be controlled and monitored. Coles and Moulton (2003), IIA (2005), ISO/IEC (2005), and Solms (2005a, 2006b) also assert that organisational security must be considered when planning for ICT risk management in an organisation.

The COBIT framework elucidates security control processes. The COBIT framework defines the elements of security control processes as: defining information architecture; defining IT organisation and relationships; managing performance and capacity; ensuring systems security; managing the configuration; managing problems; managing data; managing the physical environment; managing operations; monitoring and evaluating IT performance; and monitoring and evaluating internal control (ITGI/OGC 2005, 2008; ITGI 2007; Broderick 2006). Furthermore, the ISO/IEC 17799 standard also outlines the requirements of organisational security to ensure information security; physical and environmental security; and access control (Broderick 2006; ISO/IEC 2005). Therefore, concern with organisational information security factor can help an organisation to

achieve organisational security when dealing with ICT risk management. Ladan et al. (2006), Haworth and Pietron (2006), Myler and Broadbent (2006), Groves (2003), Karabacak and Sogukpinar (2006), Smith and McKeen (2006), Solms and Solms (2006), Solms (2005a), Westby and Allen (2007), and Byrd et al. (1995) all concur that organisational information security needs to be planned to meet information security objectives, in turn to deal effectively with ICT risk management.

Organisational information security in the case studies was referred to in both the COBIT and the ISO/IEC 17799 which outline the five indicators that measure its impact in organisations. The first indicator was examined to assess to how an organisation manages systems configuration when dealing with ICT risk management. Systems configuration concentrates on the setting of operating systems, networking operating systems, business software and hardware. The second indicator was included to evaluate how an organisation manages its access control policy when dealing with ICT risk management. Managing access control focuses on physical and environmental protection; system access; network service access; computer access; and password management systems. The third indicator was looked at to assess how an organisation handles data and information integrity management when dealing with ICT risk management. Managing data and information integrity focuses on validating data and information during input, processing and output (IPO) processes. The fourth indicator was examined to evaluate how an organisation manages security compliance when dealing with ICT risk management. Managing security compliance concentrates on ensuring security both outside (legal requirements) and inside an organisation through the implementation of rules and regulations. The fifth indicator was included to assess the extent to which an organisation monitors data protection and privacy to prevent risk when dealing with ICT risk management planning. The last indicator was looked at to assess how an organisation manages physical and environmental protection when dealing with ICT risk management.

Systems configuration; access control policy; data and information integrity management; security compliance; and data protection and privacy (six indicators) all assisted an organisation to develop an annual plan (at the corporate level) and an action plan (at the operational level) to establish successful ICT risk management (Table 6-7); thus these six indicators needed to be tested for their impact on ICT risk management in organisations.

Table 6-7: Organisational information security dimension

Proposed dimension based on the qualitative analysis	Indicator	Main concern in the COBIT framework and the ISO/IEC 17799 standard
OS		
- System configuration (Q23-Q26) - Access control policy (Q27-Q31) - Data and information integrity management (Q32-Q41)	- os1 - os2 - os3	- Organisation of information security - Access control - Security compliance

- Security compliance (Q42-Q44) - Data protection and privacy (Q45-46) - Physical and environmental protection (Q47)	- os4 - os5 - os6	- Communications - Operations management - Physical and environmental protection

Organisational information security management dimension referred to questions no. 23–47 in the questionnaire, listed as follows:

Q23. The organisation correctly configures its operating systems (e.g. Windows, Linux and Unix).

Q24. The organisation correctly configures its networking operating systems (e.g. NetWare and Cisco).

Q25. The organisation correctly configures its business software (e.g. SAP and business solution).

Q26. The organisation correctly configures its hardware (e.g. AS 400, hubs, switches, routers).

Q27. The organisation documents access control following the business requirements for system access.

Q28. The organisation allows only authorised persons to access network services.

Q29. The organisation strictly limits access to computer use by user allocation.

Q30. The organisation strictly limits access to computers by using a password management system.

Q31. The organisation monitors log files to prevent unauthorised access.

Q32. The organisation monitors computer use to prevent computer abuse.

Q33. The organisation monitors computer use in order to prevent any type of damage to information assets.

Q34. The organisation validates input data from applications systems for its correctness before inserting data into the input process.

Q35. The organisation validates input data from applications systems for its appropriateness before inserting data into the input process.

Q36. The organisation has validation check applications to detect any corruption of information through processing errors.

Q37. The organisation has validation check applications to detect any corruption of information through deliberate acts.

Q38. The organisation validates output data from applications systems for its correctness before being distributed.

Q39. The organisation validates output data from applications systems for its appropriateness before being distributed.

Q40. The organisation controls application system files in a secure manner (control of operational software).

Q41. The organisation controls application system files in a secure manner (protection of system test).

Q42. The organisation regularly checks IT facilities for compliance with security implementation standards.

Q43. All departments within the organisation have regular review plans to ensure compliance with security policy and standards.

Q44. The organisation identifies compliance with legal requirements (e.g. Thailand's *Computer Crime Act 2008*).

Q45. The organisation monitors data protection and privacy.

Q46. The organisation prevents data protection and privacy.

Q47. The organisation prevents unauthorised physical access, damage and interference to the organisation's premises and information systems.

6.3.4 Dimension four: Management of ICT resources (IT)

The area of organisational control relating to information and communication technology (ICT) and systems was raised in the six case studies. All case studies recommended that ICT and systems be reflected in the method used to manage ICT resources. In other words, ICT resources were managed through ICT management (Hinton 2006). Furthermore, the COBIT framework stipulates that ICT resources help an organisation 'to run automated business applications while leveraging business information' (ITGI 2007, p. 12). ICT resources were identified in terms of 'technology and facilities (i.e. hardware, operating system, database management system, networking, multimedia, and the environment that houses and supports them) that enable the processing of the applications' (ITGI 2007, p. 12). This view was supported by Luftman et al. (1993), McLeod and Schell (2007), McNurlin and Sprague (2006), O'Brien and Marakas (2009), and Whitman and Mattord (2009). Therefore, technology and facilities were considered

important in that they provided ICT resources in the form of networking, personal computers, software or applications, and data and information patterns.

In seeking rich information related to management of ICT resources, the COBIT framework can only be used to define the control objectives for managing ICT resources because the ISO/IEC 17799 standard is concerned more with ICT security, whereas the COBIT framework is concerned with procuring ICT resources. In relation to procuring ICT resources, it seems that all the case studies need to consider investing in new ICT resources. However, this was unlikely to occur for these organisations because they fell they have already made enough financial investments in this area; therefore, this control objective was transformed somewhat to include more of a focus on ICT resource provision instead.

There were four indicators that relate to the provision of ICT resources in an organisation. The first indicator was used to assess the extent to which an organisation provides an adequate network connection to its employees. The second indicator was included to evaluate whether an organisation provides sufficient personal access to computers for its employees. The third indicator was examined to assess how an organisation manages several types of operating software in order to generate data and information in the same file pattern. The last indicator was considered to evaluate whether an organisation provides applications with licensing.

The provision of adequate networking connections; sufficient personal access to computers; data and information patterns; and applications with licensing all assisted an organisation to plan at both the corporate level and the operational level to establish successful ICT risk management (Table 6-8); and these were therefore included for measurement in the survey.

Table 6-8: Management of ICT resources dimension

Proposed dimension based on the qualitative analysis	Indicator	Main concern in the COBIT framework
IT - Networking (Q48) - PC (Q49) - Data and information pattern (Q50) - Software (Q51)	- it1 - it2 - it3 - it4	- Management of ICT resources

Management of ICT resources dimension referred to questions no. 48–51 in the questionnaire, listed as follows:

Q48. The organisation provides an adequate networking connection to its employees.

Q49. The organisation provides sufficient personal access to computers for its employees.

Q50. The organisation manages several types of operating software in order to generate data and information in the same file pattern.

Q51. The organisation provides all applications with the required licensing.

6.3.5 Dimension five: The corporate level plan (CLP)

Planning simultaneously at both levels reflects the suggestion of Solms (2005, p. 101) to: 'Use COBIT as a "high" level reference framework in which information security governance is well positioned, and the "what" is quite clear, and use the ISO/IEC 17799 standard as a "lower" leveled guideline specifically for information security in which the "how" is more detailed'. Solms's (2005a) proposal for this 'strategic planning level' (McLeod & Schell 2007, pp. 14-15) and organisation theory (Christensen et al. 2007, p. 27) in relation to the corporate level plan of ICT risk management treatment. ICT risk management treatment arose from the case studies.

According to planning approach, ICT risk management was performed at both the corporate and operational levels in the case studies. The corporate level plan is elaborated in the treatment methodology as the scope of ICT risk management, which is then extended and translated into the operational level planning. Moreover, the analysis of case studies revealed that different management level staff are concerned that the planning stage is separated in this way, arguing instead that the overall plan must be developed through consensus agreement.

In order to link this dual-level planning, this study proposed four indicators to explain the corporate level planning factor. The first indicator was used to evaluate the extent to which an organisation conducts ICT risk management based on the direction and control from the management level through a top-down approach. The second indicator was included to evaluate the extent to which an organisation establishes ICT control and audit in its annual plan to meet organisational objectives. The third indicator was considered to evaluate whether an organisation provides an overview of ICT applications and information security in its ICT plan. The last indicator was included to assess whether an organisation provides an overview of its ICT risk management methodology.

Management direction and control (a top-down approach); establishing ICT control and an ICT audit plan in the corporate plan; providing an overview of ICT application and information security in the ICT plan; and providing an overview of ICT risk management methodology can all assist an organisation to supplement its operational plan to establish successful ICT risk management (Table 6-9); thus these were included for measurement in the survey.

Table 6-9: The corporate level plan dimension

Proposed dimension based on the qualitative analysis	Indicator	Main concern in the COBIT framework and the ISO/IEC 17799 standard
CLP - Top-down approach (Q11) - ICT control and audit (the corporate plan) (Q52) - IT plan (Q53) - ICT risk management methodology (Q54)	- clp1 - clp2 - clp3 - clp4	- The corporate level plan - Strategy direction (top-down) - IT governance (ICT processes)

The corporate level plan dimension referred to questions no. 11 and 52–54 in the questionnaire, listed as follows:

Q11. The organisational strategies in ICT risk management are generated by management.

Q52. The organisation has established IT control and audit in the corporate plan to reflect the organisation objectives.

Q53. The organisation provides an overview of IT applications and IT security in its IT plan.

Q54. The organisation provides an overview of its ICT risk management methodology.

6.3.6 Dimension six: The operational level plan (OLP)

The operational level plan reflects the recommendations of Solms (2005a) regarding 'the strategic planning level' (McLeod & Schell 2007, pp. 14-15). The operational level plan also relates to ICT risk management treatment as discussed in the case studies. The overall ICT plan at the corporate level is communicated down to, and directs, the operational plan. This operational level plan focuses on a bottom-up approach to ICT risk management which elucidates the details of ICT project risk management specific to each department within an organisation. This plan is vital for operations in terms of providing and covering the details of internal information that a corporate level plan is not able to incorporate (McLeod & Schell 2007). The connection between the operational level plan and the corporate level plan lies in the collaborative planning between both levels to reach an organisation-wide ICT risk management plan.

In order to align the operational level plan with the corporate level plan, this research identified four indicators that contribute to an understanding of how the bottom-up approach aligns with the top-down approach to represent both as an enterprise-level plan. The first indicator was included to assess how an organisation directs and controls ICT risk management through the operational level or a bottom-up approach. The second

indicator was examined to assess the extent to which an organisation establishes information security control and audit in its action plan for specific departments. The third indicator was looked at to assess whether an organisation defines information security in its operational plan. The last indicator was included to estimate whether an organisation outlines ICT project risk management methodology for a specific project.

Operation direction and control (a bottom-up approach); establishing information security control and information security audit; defining information security in its security plan; and providing ICT risk project management methodology for a specific project all enable an organisation to supplement its corporate level plan in order to establish successful ICT risk management (Table 6-10); thus these four indicators need to be tested in the survey.

Table 6-10: The operational level plan dimension

Proposed dimension based on the qualitative analysis	Indicator	Main concern in the COBIT framework and the ISO/IEC 17799 standard
OLP - Bottom-up approach (Q12) - Information security control and information security audit (the action plan) (Q55) - IT security plan (Q56) - ICT project risk management methodology (Q57)	- olp1 - olp2 - olp3 - olp4	- The operational level plan - Strategy direction (bottom-up) - IS governance (IS processes)

The operational level plan dimension referred to questions no. 12 and 52–54 in the questionnaire, listed as follows:

Q12. The organisational strategies in ICT risk management are generated at the operational level.

Q55. The organisation has established information security control and audit in its action plan for specific departments.

Q56. The organisation provides information security in security direction.

Q57. The organisation provides IT project risk management methodology for specific projects.

6.3.7 Dimension seven: Successful ICT risk management (SICTRM)

The objective of ICT risk management is to mitigate, prevent and avoid ICT risks, and their negative impact and potential for loss (refer to Chapter 2, p. 23 and Table 6-11 below).

Table 6-11: Successful ICT risk management dimension

Proposed dimension based on the qualitative analysis	Indicator	Main concern based on the literature
SICTRM - Mitigate ICT risks to an acceptable level (Q58) - Prevent ICT risks (Q59) - Avoid ICT risks (Q60)	- sictrm1 - sictrm2 - sictrm3	- Successful ICT risk management (refer to the objective of ICT risk management in Chapter 2)

Successful ICT risk management dimension referred to questions no. 58–60 in the questionnaire, listed as follows:

Q58. Successful ICT risk management helps the organisation mitigate ICT risks to risk appetites (acceptable level).

Q59. Successful ICT risk management helps the organisation prevent ICT risks appropriately.

Q60. Successful ICT risk management helps the organisation avoid ICT risks appropriately.

After all constructs were generated, the conceptual model was developed, which is outlined next.

6.3.8 The conceptual model

In order to confirm the findings, a conceptual model was generated in this chapter and was then tested in the quantitative data analysis (refer to Chapter 7). The qualitative study proposed that organisational policy; human resource management and planning; organisational security; and management of ICT resources positively affect planning at both the corporate level and the operational level when establishing successful ICT risk management (Figure 6-1). The conceptual model, based on this tenet, derived from the case study research and existing literature, was then hypothesised, that 'the conceptual model of successful ICT risk management positively influences success factors of ICT risk management in Thai businesses' (Wright 1923). Wright (1923, p. 241) states that 'finding the logical consequences of a hypothesis in regard to the causal relationships does not depend on any prior assumption that the hypothesis is correct. Neither does it imply that the theory of path coefficients by itself gives a method of proving such a hypothesis. It does, of course, follow that if one of the logical consequences of a hypothesis is absurd the hypothesis is untenable and must be modified; on the other hand, if the logical consequences can be shown to agree with independently obtained results it contributes to the demonstration of the truth of the hypothesis in the only sense which can be ascribed to the truth of a natural law'. Each path presents causal

relations to a system (i.e. the conceptual model) regardless of 'whatever knowledge may be possessed or whatever hypothesis it is desired to test as to causal relations' (Wright 1922, p. 255). Therefore, this research hypothesised only the model which presents a system of successful ICT risk management.

The hypothesis concerned the whole model, rather than only parts of it, because this model represented the whole system of successful ICT risk management (each key factor affects successful ICT risk management) rather than individual paths or relationships in the model.

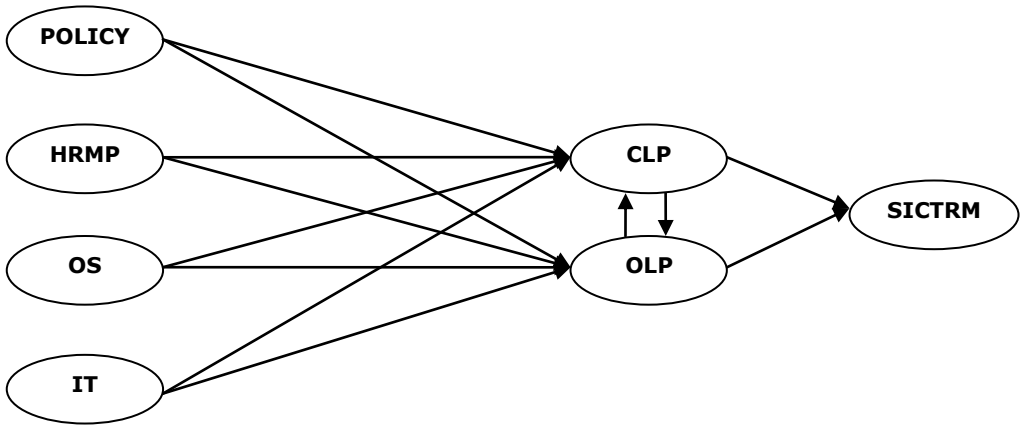


Figure 6-1: The conceptual model of successful ICT risk management

6.4 Conclusion

ICT risk management in these six case studies of Thai businesses was focused at both the corporate and operational levels. The corporate level set the overall ICT risk management plan. The operational level covered the specific technical security plan for ICT, defined as ICT project risk management. Furthermore, both the corporate and the operational levels in the six organisations revealed that organisational policy; human resource management and planning; organisational information security management; and management of ICT resources were the main factors to be considered when dealing with successful ICT risk management.

In order to successfully achieve ICT risk management, the six case studies revealed that these organisations concentrate on general ICT and ICT security simultaneously. The six companies recommended that the two approaches be linked to form a complete pipeline (a two-way approach) in seeking to attain effective ICT risk management. The two-way approach worked well as the COBIT framework laid the foundation for a top-down approach to risk management, while the ISO/IEC 17799 standard focused on the bottom-up approach to risk management. Furthermore, the discussion indicates that organisational structure, organisational control, organisational process and organisational

ICT strategy evaluated in these six case studies reflected use of both the COBIT framework and the ISO/IEC 17799 standard, and it was reported that the organisations perceive them both to be effective and efficient in keeping risks under control.

The next chapter discusses further how ICT risk management can be applied in an organisation. The effective key factors (revealed by the qualitative analysis) for ICT risk management are compared with the COBIT framework and the ISO/IEC 17799 standard in order to propose success factors for inclusion in successful ICT risk management, to test the relationships and confirm the qualitative findings through quantitative analysis.

Chapter 7

SURVEY ANALYSIS

This chapter presents an analysis of the data derived from the survey of ICT risk management in Thai organisations. The data collection method used is based on the propositions and dimensions developed from the findings of the qualitative study of ICT risk management in six Thai businesses (refer to Chapters 4, 5 and 6). Through structural equation modelling (SEM), the conclusions derived from Chapter 6 are tested, validated and confirmed in this chapter in order to propose a model of successful ICT risk management (SICTRM). The chapter begins with screening data followed by a discussion of the validity and reliability of the instrument. The chapter concludes by proposing success factors for dealing with ICT risk management planning in order to mitigate, prevent and avoid ICT risks (Figure 7-1).

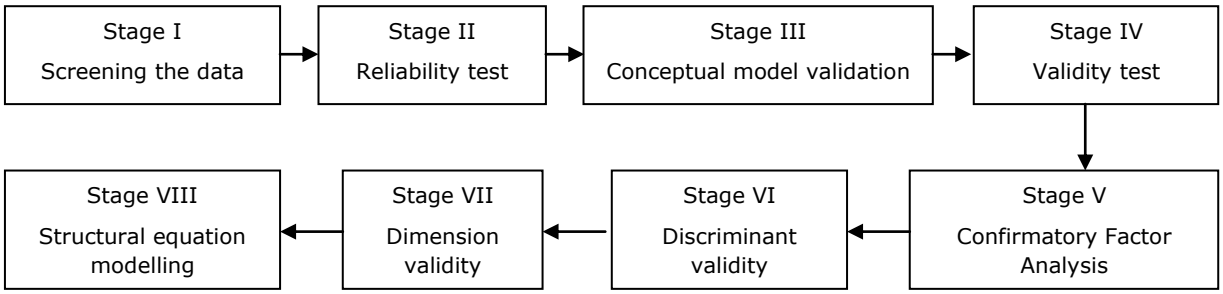


Figure 7-1: A flowchart of model validation

7.1 Demographic statistics

The survey included 302 respondents who worked in the field of ICT risk management in organisations (Table 7-1). Of the respondents, 44.7% were from banking, 36.1% were from telecommunications, and 19.2% were from insurance. The largest proportion of position levels were in operations at 59.3%, while the remaining 40.7% were from management levels. Staff from IT departments returned the survey at the largest rate of 34.8%, followed by 22.8% from internal audit departments, 19.2% from finance and

accounting departments, and 15.2% from information security departments. Surprisingly, staff from risk management departments returned the survey at the lowest rate of 7.9%, although risk management was the main responsibilities of their work. The next section discusses the response rate of this research

Table 7-1: Demographic statistics

Type of Business	Frequency	Percentage
Bank	135	44.7
Telecommunications	109	36.1
Insurance	58	19.2
Total	302	100.0
Position Level		
Management	123	40.7
Operational	179	59.3
Total	302	100.0
Department		
Information Technology	105	34.8
Internal Audit	69	22.8
Finance and Accounting	58	19.2
Information Security	46	15.2
Risk Management	24	7.9
Total	302	100.0

7.2 Survey response rate

As discussed in Chapter 3 (p. 67) stratified random sampling was selected because a stratified sample helped the researcher to focus on only those organisations that are familiar with managing ICT risks. The population was comprised of 497 organisations listed on the Stock Exchange of Thailand (SET). The stratified sample exemplars (55 out of the total 497 listed organisations) were selected from an analysis of organisational structure regarding ICT infrastructure in combination with organisation reports to the SET. The sample was stratified by type of business: banking, telecommunications or insurance. Eleven banking, 25 telecommunications, and 17 insurance companies were included. One thousand surveys were sent out to potential respondents to participate in this research, from which 302 surveys were returned. Thus, the response rate is equal to:

$$\text{Total response rate} = \frac{302 \times 100}{1{,}000} = 30.20\%$$

As a result of the stratified random sampling, the sample number was limited to improve the response rate, although this data collection was conducted by using survey techniques based on subject interest, prepaid postage, multiple mailing and pre-tested surveys (Frohlich 2002).

7.3 Item parcelling

Conway and Huffcutt (2003), Cook (1981), Fabrigar et al. (1999), Gerbing and Anderson (1985), Gorsuch (1983), and Tabachnick and Fidell (2007) argue that the number of items per dimension should be made up of between three to five indicators. Furthermore, the sample size of this research (302) can be considered small in so far as Bentler and Chou (1987), and Baumgartner and Homburg (1996, p. 146) suggest in regard to samples per indicator that 'the ratio of sample size to number of free parameters should be at least 5:1 to get trustworthy parameter estimates, and they further suggest that these ratios should be higher (at least 10:1, say) to obtain appropriate significance tests'. Therefore, a number of indicators were considered in this research to ensure the tests were conducted properly.

This research follows the above suggestion pertaining to the recommended number of indicators per dimension (Baumgartner & Homburg 1996). The questions in the survey were produced using the proposed indicators as key elements. For example, the indicators in Human resource management and Planning (HRMP, Chapter 6, p. 154) and Organisational ICT Security (OS, Chapter 6, p. 156) cannot be clearly explained in isolation (refer to Appendix B5 and B6). They were expanded into several questions in order to facilitate better understanding of the question/item and indicators. However, the items in each dimension exceeded the preferred ratio of sample size to number of indicators in this research. Therefore, they had to be reduced in order to meet the grounded indicator and the dimension based on the proposed indicators from Chapter 6 (HRMP, p. 154 and OS, p. 156). Moreover, the reduction of the number of indicators leads to the small sample size requirement for the study. Three hundred and two samples are considered to be a small sample size (Bentler & Chou 1987; Baumgartner & Homburg 1996). Item parcelling was then used to reduce the number of indicators in order to signify the model in the structural equation modelling (SEM) properly. The main reason for having a large sample size is that 'all methods for the estimation and testing of structural equation models are based on asymptotic theory and the sample size has to be "large" for the parameter estimates and test statistics to be valid' (Baumgartner & Homburg 1996, p. 146).

Nasser and Takahashi (2003, p. 76) assert that 'item parcelling is used to reduce model complexity and to reduce the number of parameters estimated without researchers' having to pay the price of eliminating items and losing information that may contribute to

the meaning of a latent variable'. Moreover, Little et al. (2002, p. 152) argue that 'parcelling is a measurement practice that is used most commonly in multivariate approaches to psychometrics, particularly for use with latent-variable analysis techniques (e.g. Structural Equation Modelling-SEM)'.

Item parcelling in this research was performed to reduce the number of indicators in a latent variable in order to meet the small sample size of this research. The reason for the use of item parcelling is that some rules of thumb for determining adequate sample size are based on the ratio of estimated parameters to respondents (Hall et al. 1999). In doing so, some theorists suggest that item parcelling is performed by calculating average means of all items to represent the new mean for the new indicator (Cattel & Burdsal 1975; Bandolos & Finney 2001; Enders & Bandalos 1999; Hall et al. 1999; Yuan et al. 1997; Marsh et al. 1988; Nasser & Takahashi 2003). This suggestion is considered when reducing a number of indicators and is performed only for the indicators among the dimensions that exceed five indicators in order to meet the required ratio of sample to indicator (Baumgartner & Homburg 1996).

There were two dimensions (HRMP and OS) that contained items (questions) of more than five items per indicator. The HRMP dimension is the first dimension, for which 10 items needed to be reduced to match the original four indicators (Table 7-2). Item parcelling was carried out using the Transform Menu in the Compute Variable Function in the Statistical Package for the Social Sciences (SPSS V 16), as shown in the Syntax below (Figure 7-2).

```
COMPUTE hrmp1=mean(q13,q14,q15,q16).
EXECUTE.
COMPUTE hrmp2=mean(q17,q18).
EXECUTE.
COMPUTE hrmp3=mean(q19,q20)
EXECUTE.
COMPUTE hrmp4=mean(q21,q22).
EXECUTE.
```

Figure 7-2: Syntax of parcelling computation of HRMP

According to Figure 7-2, for example, the average means of items (q13-q16) were computed to represent the new mean for the new indicator (hrmp1). The new given name of each indicator followed from the dimension name along with a number of indicators as hrmp1, hrmp2, hrmp3 and hrmp4, represented in Table 7-2 below.

Table 7-2: Human resource management and planning dimension (repeated from Table 6-6)

Proposed dimension based on the qualitative analysis	Indicator	Main concern in the COBIT framework and the ISO/IEC 17799 standard
HRMP		
- Roles and responsibilities (Q13-Q16) - Human resources protection (Q17-Q18) - Training and education (Q19-Q20) - Human resources security (Q21-Q22)	- hrmp1 - hrmp2 - hrmp3 - hrmp4	- Organisational control of people - HR access control and protection - Educating and training users - Human resources security

The Organisational ICT Security (OS) dimension is the second dimension, for which 24 items needed to be reduced to match with the original five indicators (Table 7-3). Item parcelling was carried out using the Transform menu in the compute variable function in the Statistical Package for the Social Sciences (SPSS V 16), as shown in the Syntax below (Figure 7-3).

```
COMPUTE os1=mean(q23,q24,q25,q26).
EXECUTE.
COMPUTE os2=mean(q27,q28,q29,q30,q31).
EXECUTE.
COMPUTE os3=mean(q32,q33,q34,q35,q36,q37,q38,q39,q40,q41).
EXECUTE.
COMPUTE os4=mean(q42,q43,q44).
EXECUTE.
COMPUTE os5=mean(q45,q46).
EXECUTE.
```

Figure 7-3: Syntax of parcelling computation of OS

The new given name of each indicator followed from the dimension name along with a number of indicators as os1, os2, os3 and os4 and os5, represented in Table 7-3.

Table 7-3: Organisational information security dimension (repeated from Table 6-7)

Proposed issue based on the qualitative analysis	Indicator	Main concern in the COBIT framework and the ISO/IEC 17799 standard
OS		
- System configuration (Q23-Q26) - Access control policy (Q27-Q31) - Data and information integrity management (Q32-Q41) - Security compliance (Q42-Q44) - Data protection and privacy (Q45-46) - Physical and environmental protection (Q47)	- os1 - os2 - os3 - os4 - os5 - os6	- Organisation of information security - Access control - Security compliance - Communications - Operations management - Physical and environmental protection

After undertaking item parcelling, the number of items (and the number of questions in the questionnaire) was reduced to match with the original indicators in each dimension. Each dimension was then ready for validation in the next stage.

7.4 Stage I: Descriptive analysis of the questionnaire

Based on the questionnaire dimensions, the subsections are discussed dependent upon the descriptive analysis (Figure 7-4) of the questionnaire, focusing on each item alongside the information.

```
DESCRIPTIVES VARIABLES=policy1 policy2 policy3 policy4 hrmp1 hrmp2
hrmp3 hrmp4 os1 os2 os3 os4 os5 os6 it1 it2 it3 it4 clp1 clp2 clp3 clp4
olp1 olp2 olp3 olp4 sictrm1 sictrm2 sictrm3
/STATISTICS=MEAN STDDEV.
```

Figure 7-4: Syntax of the descriptive analysis of all indicators

Organisational policy (POLICY)

The results of the analysis of the mean of each indicator in the POLICY dimension ranged from 5.71 to 5.94 (see Table 7-4). This indicates that respondents generally agreed with the statement that the organisation defines ICT policy and Information security policy alongside a risk statement and a business continuity plan. All indicators were required to deal with ICT risk management.

Table 7-4: An analysis of the mean of the POLICY dimension

Descriptive Statistics				
Dimension/Dimension		N	Mean	Std. Deviation
Organisational Policy (POLICY)				
IT objectives−policy1 (Q7)		302	5.83	1.197
IS objectives−policy2 (Q8)		302	5.94	1.197
Risk statement−policy3 (Q9)		302	5.71	1.367
Business continuity plan−policy4 (Q10)		302	5.93	1.252
	policy1	policy2	policy3	policy4
Chi-Square	280.205	321.232	240.848	3.270E2
Df	6	6	6	6
Asymp. Sig.	0.000	0.000	0.000	0.000

Human resource management and planning (HRMP)

Four indicators related to the HRMP dimension, and the results of the analysis of the mean ranged from 5.48 to 6.25 (see Table 7-5). This result reflects that respondents generally agreed with the statement that the organisation pays attention to HRMP especially in terms of human resources security (termination or change of employment).

Table 7-5: An analysis of the mean of the HRMP dimension

Descriptive Statistics				
Dimension/Dimension		N	Mean	Std. Deviation
Human resource management and Planning (HRMP)				
Roles and responsibilities−hrmp1 (Q13-Q16)		302	5.48	1.332
Human resources protection−hrmp2 (Q17-Q18)		302	5.95	1.215
Training and education−hrmp3 (Q19-Q20)		302	5.90	1.225
Human resources security−hrmp4 (Q21-Q22)		302	6.25	1.077
	hrmp1	hrmp2	hrmp3	hrmp4
Chi-Square	511.298	581.656	643.212	686.543
df	23	12	12	10
Asymp. Sig.	0.000	0.000	0.000	0.000

Organisational ICT Security (OS)

In this dimension, the results of the analysis of the mean ranged from 5.90 to 6.22 (see Table 7-6). This illustrates that respondents generally agreed with the statement that the organisation pays attention to organisational security, especially during the planning stage for physical and environmental protection.

Table 7-6: An analysis of the mean of the OS dimension

Descriptive Statistics						
Dimension/Dimension				N	Mean	Std. Deviation
Organisational information Security (OS)						
System configuration−os1 (Q23-Q26)				302	5.94	1.098
Access control policy−os2 (Q27-Q31)				302	6.09	1.009
Data and information integrity management−os3 (Q32-Q41)				302	5.90	1.039
Security compliance−os4 (Q42-Q44)				302	5.92	1.127
Data protection and privacy−os5 (Q45-Q46)				302	5.88	1.226
Physical protection−os6 (Q47)				302	6.22	1.135
	os1	os2	os3	os4	os5	os6
Chi-Square	815.550	589.219	622.073	519.205	528.702	513.430
df	17	21	42	17	11	6
Asymp. Sig.	0.000	0.000	0.000	0.000	0.000	0.000

Management of information and communication technology resources (IT)

In this dimension, the results of the analysis of the mean ranged from 6.02 to 6.11 (see Table 7-7). These findings indicate that respondents generally supported the view that the organisation provides sufficient ICT resources to its staff and manages them in a proper way.

Table 7-7: An analysis of the mean of the IT dimension

Descriptive Statistics			
Dimension/Dimension	N	Mean	Std. Deviation
Information and Communication Technology Resources Management (ICT)			
Sufficient networking connection–it1 (Q48)	302	6.02	1.174
Sufficient personal computer–it2 (Q49)	302	6.11	1.240
Same file pattern–it3 (Q50)	302	6.03	1.079
Applications with licensing–it4 (Q51)	302	6.10	1.080

	it1	it2	it3	it4
Chi-Square	366.662	447.325	361.470	398.278
df	6	6	6	6
Asymp. Sig.	0.000	0.000	0.000	0.000

The corporate level plan (CLP)

Under this dimension, the results of the analysis of the mean ranged from 5.75 to 5.93 (see Table 7-8). This reveals that respondents generally supported the views: firstly, that the CLP in the organisation includes the details regarding ICT control and audit planning in its annual plan; secondly, that the CLP in the organisation includes an overview of ICT applications and ICT security in the organisation's ICT plan; and lastly, that the CLP in the organisation guides ICT risk management methodology through a top-down approach (refer to Chapters 4 and 5).

Table 7-8: An analysis of the mean of the CLP dimension

Descriptive Statistics			
Dimension/Dimension	N	Mean	Std. Deviation
The Corporate Level Plan (CLP)			
Top-down approach–clp1 (Q11)	302	5.75	1.313
ICT control and audit in the corporate plan–clp2 (Q52)	302	5.90	1.167
ICT applications and ICT security overview in the ICT plan–clp3 (Q53)	302	5.93	1.192
ICT risk management methodology–clp4 (Q54)	302	5.88	1.168

	clp1	clp2	clp3	clp4
Chi-Square	267.132	219.364	320.397	300.510
df	6	5	6	6
Asymp. Sig.	0.000	0.000	0.000	0.000

The operational level plan (OLP)

In this dimension, the results of the analysis of the mean ranged from 5.63 and 5.73 (see Table 7-9). This indicates that respondents generally supported the view that: firstly, the OLP in the organisation outlines the details regarding information security control and audit; secondly, the OLP guides the outline of the information security plan; and lastly, that ICT project risk management methodology is provided in the OLP as part of a bottom-up approach in an organisation (refer to Chapters 4 and 5).

Table 7-9: An analysis of the mean of the OLP dimension

Descriptive Statistics			
Dimension/Dimension	N	Mean	Std. Deviation
The Operational Level Plan (OLP)			
Bottom-up approach–olp1 (Q12)	302	5.63	1.374
IS control and audit in the action plan–olp2 (Q55)	302	5.73	1.265
ICT Security plan–olp3 (Q56)	302	5.66	1.335
ICT project risk management methodology–olp4 (Q57)	302	5.67	1.305

	olp1	olp2	olp3	olp4
Chi-Square	241.728	256.702	244.417	234.821
df	6	6	6	6
Asymp. Sig.	0.000	0.000	0.000	0.000

Successful ICT risk management (SICTRM)

The results of the analysis of the mean in indicators of the SICTRM dimension ranged between 6.01 and 6.04 (see Table 7-10). These findings show that respondents generally agreed with the statement that successful ICT risk management can help an organisation mitigate, prevent and avoid ICT risk.

Table 7-10: An analysis of the mean of the SICTRM dimension

Descriptive Statistics			
Dimension/Dimension	N	Mean	Std. Deviation
Successful ICT Risk Management (SICTRM)			
Mitigating ICT risks–sictrm1 (Q58)	302	6.01	1.083
Preventing ICT risks–sictrm2 (Q59)	302	6.04	.972
Avoiding ICT risks–sictrm3 (Q60)	302	6.02	1.000

	sictrm1	sictrm2	sictrm3
Chi-Square	349.742	274.238	161.079
df	6	5	4
Asymp. Sig.	0.000	0.000	0.000

After screening the data, all indicators and dimensions were shown to be significant and ready to validate in the next step, prior to carrying out the structural equation modelling.

7.5 Stage II: Reliability testing

Reliability is referred to as an 'issue of measurement within a dimension and a statement about measurement accuracy' (Cronbach 1951 in Straub et al. 2004, p. 36). According to Hair et al. (2006), Cronbach's Alpha provides internal consistency of the scale that measures the reliability of an index of instrument stability. A high value for Cronbach's Alpha indicates that the reliability of an instrument is also high.

According to the rule of thumb of Nunnally (1978, 1967), the value of Cronbach's Alpha is acceptable when it is greater than .60 for internal consistency for exploratory research or .70 for internal consistency for confirmatory research (Straub et al. 2004). Thus, Cronbach's Alpha was used to validate the reliability of a psychometric test score for a sample of respondents in this research. The Cronbach's Alpha values of all dimensions were estimated using SPSS V 16.

The Cronbach's Alpha values are shown in Table 7-11 below. The results show that Cronbach's Alpha coefficient scores ranged from .904 to .942 across the factors.

Table 7-11: Reliability of indicators within the instrument

Factor	Indicator	Cronbach's Alpha
POLICY	policy1 policy2 policy3 policy4	.924
HRMP	hrmp1 hrmp2 hrmp3 hrmp4	.904
OS	os1 os2 os3 os4 os5 os6	.942
IT	it1 it2 it3 it4	.918
CLP	clp1 clp2 clp3	.909

	clp4	
OLP	olp1 olp2 olp3 olp4	.912
SICTRM	sictrm1 sictrm2 sictrm3	.939
All		.976

Entire indicators within the dimension are greater than .60 for exploratory research (Chapter 3, p. 57). Therefore, the results demonstrate good reliability of internal consistency.

7.6 Stage III: Validating the conceptual model

According to the conceptual model, based on the tenet derived from the case study research and existing literature, it is hypothesised that 'the conceptual model of successful ICT risk management positively influences success factors of ICT risk management in Thai businesses' (repeated in Chapter 6, p. 163). The hypothesis concerns the whole model, rather than only its parts, because this model represents the whole system of successful ICT risk management (each key factor affects successful ICT risk management) rather than individual paths or relationships in the model.

The conceptual model estimated the values of indices of Structural Equation Modelling (SEM). The values of indices were as follows: χ^2/df (2054.711/366)=5.614, p=.002, TLI=.810, CFI=.829, RMSEA=.124, SRMR=.416, and HOELTER=61 with a confidence level of 95%, as shown in Table 7-12 and Figure 7-5. All indices values demonstrate that the conceptual model does not present the perception of the sample.

Table 7-12: Conceptual model of successful ICT risk management in SEM

Cut-off value		Model Fit
Indices	Required Value	
χ^2/df (2054.711/366)	< 3	5.614
P-value	> .05	.002
TLI	≥ .95	.810
CFI	≥ .95	.829
RMSEA	< .06	.124
SRMR	< .08	.416
HOELTER (P=0.05)	≥ 200	61

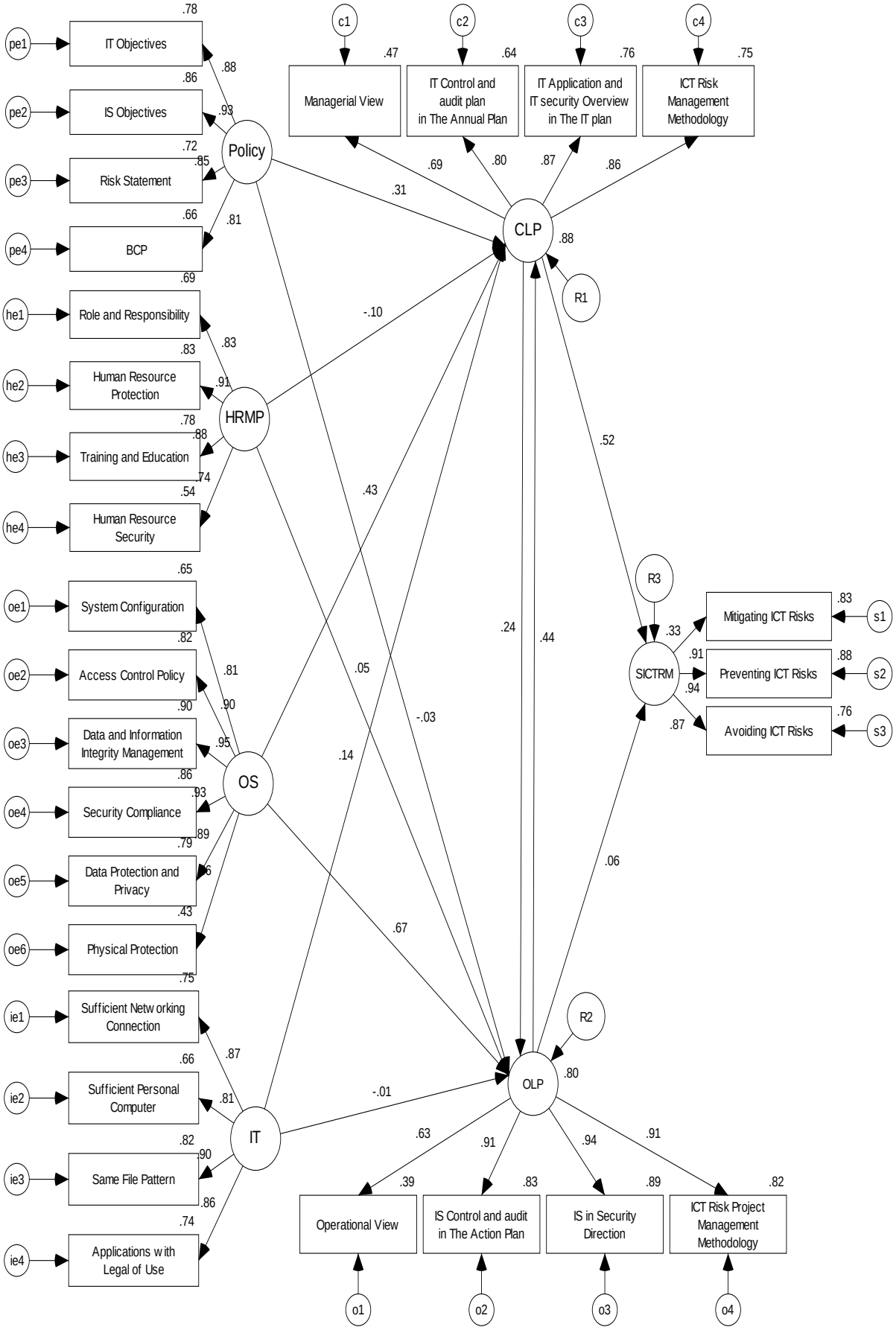


Figure 7-5: The conceptual model validation

Based on the results of the conceptual model, the values of all dimensions were found to be non-significant. From there, the other three analytical processes could be carried out. Firstly, the factor loading was used to evaluate how items could accurately explain a factor. The factor loadings of indicators should be greater than 0.7 (Hair et al. 2006). Therefore, the factor loadings of all indicators in all dimensions were statistically estimated, the results of which are presented in Table 7-13. The factor loadings of three indicators—os6: Physical Protection in Organisational Information Security (OS) dimension, clp1: the Managerial View in the Corporate Level Plan (CLP) dimension, and olp1: the Operational view in the Operational Level Plan (OLP)—were found to be less than 0.7 (see Table 7-13). This demonstrates that these three indicators do not sufficiently explain the factors.

Table 7-13: Standardised regression weights: The conceptual model

Item	Path	Item	Estimate	Item	Path	Item	Estimate
CLP	<---	OLP	.444	oc6	<---	OS	.659
CLP	<---	POLICY	.313	os5	<---	OS	.891
CLP	<---	OS	.433	os4	<---	OS	.926
CLP	<---	IT	.136	os3	<---	OS	.951
CLP	<---	HRMP	-.095	os2	<---	OS	.904
OLP	<---	CLP	.237	os1	<---	OS	.809
OLP	<---	HRMP	.047	it4	<---	IT	.858
OLP	<---	IT	-.011	it3	<---	IT	.903
OLP	<---	POLICY	-.025	it2	<---	IT	.813
OLP	<---	OS	.668	it1	<---	IT	.867
SICTRM	<---	OLP	.059	clp4	<---	CLP	.865
SICTRM	<---	CLP	.523	clp3	<---	CLP	.872
policy4	<---	POLICY	.815	clp2	<---	CLP	.803
policy3	<---	POLICY	.849	clp1	<---	CLP	.689
policy2	<---	POLICY	.927	olp4	<---	OLP	.907
policy1	<---	POLICY	.884	olp3	<---	OLP	.942
hrmp4	<---	HRMP	.735	olp2	<---	OLP	.911
hrmp3	<---	HRMP	.882	olp1	<---	OLP	.628
hrmp2	<---	HRMP	.911	sictrm1	<---	SICTRM	.909
hrmp1	<---	HRMP	.831	sictrm2	<---	SICTRM	.937
				sictrm3	<---	SICTRM	.873

Secondly, the estimation of the Critical Ratio (C.R.) values in each dimension and each indicator was also undertaken to evaluate the significance of the relationships between the dimensions. C.R. or path coefficient (see Table 7-14) in each path should be greater than 1.96 for a regression weight, and that path is significant at the 95% confidence interval (that is, its estimated path parameter is significant) (Garson 2009). Table 7-14 shows the coefficient or CR values of the four paths which are: Human resource

management and Planning (HRMP) and the Operational Level Plan (OLP); Management of ICT resources (IT) and the Operational Level Plan (OLP); Organisational Policy (POLICY) and the Operational Level Plan (OLP); and the Operational Level Plan (OLP) and Successful ICT risk management. The coefficient values of the four paths were less than 1.96, and the p-values of the four paths were greater than 0.05, indicating that the four paths were insignificant at the 95% confidence interval (see Table 7-14).

Table 7-14: Regression weights: The conceptual model

			C.R.	P	Item	Path	Item	C.R.	P
CLP	<---	POLICY	8.244	***	oc6	<---	OS	14.064	***
CLP	<---	OS	6.404	***	os5	<---	OS	25.891	***
CLP	<---	IT	4.299	***	os4	<---	OS		
CLP	<---	HRMP	-3.064	.002	os3	<---	OS	32.157	***
CLP	<---	OLP	7.955	***	os2	<---	OS	27.074	***
OLP	<---	CLP	7.955	***	os1	<---	OS	20.393	***
OLP	<---	HRMP	1.490	.136	it4	<---	IT		
OLP	<---	IT	-.354	.724	it3	<---	IT	20.752	***
OLP	<---	POLICY	-.748	.454	it2	<---	IT	17.476	***
OLP	<---	OS	13.143	***	it1	<---	IT	19.463	***
SICTRM	<---	OLP	.492	.623	clp4	<---	CLP	13.884	***
SICTRM	<---	CLP	4.187	***	clp3	<---	CLP	13.992	***
policy4	<---	POLICY			clp2	<---	CLP	12.980	***
policy3	<---	POLICY	17.510	***	clp1	<---	CLP		
policy2	<---	POLICY	19.876	***	olp4	<---	OLP		
policy1	<---	POLICY	18.582	***	olp3	<---	OLP	28.265	***
hrmp4	<---	HRMP			olp2	<---	OLP	25.722	***
hrmp3	<---	HRMP	15.338	***	olp1	<---	OLP	12.780	***
hrmp2	<---	HRMP	15.764	***	sictrm1	<---	SICTRM		
hrmp1	<---	HRMP	14.420	***	sictrm2	<---	SICTRM	25.957	***
					sictrm3	<---	SICTRM	22.536	***

Lastly, the modification indices (MIs) were also used to represent the highest covariance values, which suggested that the indicators related to misspecification (Byrne 2001; Hair et al. 2006) between two variables, as shown in the list of MIs in Table 7-15. All dimensions were conceptualised according to the relationships within the conceptual model based on the qualitative analysis. Table 7-15 shows the highest covariance values between two variables or dimensions (i.e. HRMP <--> OS, POLICY <--> OS, OS <--> IT, HRMP <--> IT, POLICY <--> IT and POLICY <→ HRMP) which related to the misspecification of the relationships in the conceptual model.

Table 7-15: Covariances: The conceptual model

			M.I.	Parameter Change
HRMP	<-->	OS	204.373	.719
POLICY	<-->	OS	170.365	.839
OS	<-->	IT	167.267	.760
HRMP	<-->	IT	111.637	.483
POLICY	<-->	IT	94.323	.567
POLICY	<-->	HRMP	149.610	.611

On the basis of these results, the conceptual model was rejected. Then the structural equation modelling was used to modify the successful ICT risk management model. The modification stage was aimed at representing the success factors for ICT risk management in Thai businesses. The development of the successful ICT risk management planning model commenced with validity testing, which is presented in the following section.

7.7 Stage IV: Validity testing and model analysis

Content and construct validity tests were used to represent the degree of accuracy between a set of measures and the concept of interest (Cronbach & Meehl 1955; Hair et al. 2006). Construct or dimension validity testing was used to evaluate the model fit through structural equation modelling (SEM) in this research.

SEM is a powerful statistical tool that enables the researcher to address a wide range of managerial and theoretical questions (Hair et al. 2006). SEM is a widely accepted method of evaluating dimension validity and the theoretical relationship among dimensions or factors (Hair et al. 2006; Kline 2005). SEM is used to validate multiple dependent variables (dimensions or factors) such as multivariate analysis of variance to represent a single relationship between the dependent and independent variables (Hair et al. 2006).

Analysing the data in this research through SEM, a four-step modelling process based on Mulaik and Millsap's (2000) suggestion was conducted. Firstly, the number of factors (latent) is normally established by using exploratory factor analysis (EFA), to validate the indicators for each factor. However, in this research EFA was not considered suitable because Hair et al. (2006) suggest that EFA is not needed when the dimension is conceptualised with the theoretical concept as measurement theory. Moreover, Byrne (2001, p. 5) adds that 'EFA is designed for the situation where links between the observed (the measures or items) and latent variables (the dimensions) are unknown or

uncertain'. All dimensions in this research were developed based on the literature, the COBIT framework and the ISO/IEC 17799 standard, which are internationally accepted; therefore, all dimensions were already known and certain. Hair et al. (2006, p. 799) also state that 'CFA is a special type of factor analysis and is the first part of a complete test of a structural model in SEM. Unlike EFA, the researcher must be able to tell the SEM program which variables belong with which factor before an analysis can be conducted'.

For all dimensions in this research, it was known in advance which variables belonged with which factors or dimensions prior to conducting the analysis (refer to discussion of the conceptual model in Chapter 6, p. 163). Therefore, EFA was not considered necessary in this research. If a pair of dimensions was recommended to combine as one dimension because of a lack of discriminant validity, then EFA was used to evaluate that all indicators represent the similar intended perspective. In doing so, EFA was used to reconfirm that both two constructs really represented the content similarity or the construct similarity. Afterward, both two constructs was then combined to represent only one construct.

The second step recommended by Mulaik and Millsap (2000) is confirmatory factor analysis (CFA). CFA was used in this research to confirm the indicators within the factors by using factor loadings to justify whether each indicator should be dropped or retained for each factor. CFA was used to validate dimension validity which includes convergent, discriminant and nomological validities (Campbell & Fiske 1959; Hair et al. 2006). Three types of validation known as dimension validity are explained in detail in the next section.

Mulaik and Millsap's (2000) third stage entails development of a structural model. A structural model was therefore established in this research to confirm the hypothesis and the relationship among factors, and then used to propose the success factors of ICT risk management.

The final stage of Mulaik and Millsap's (2000) approach is a nested model test. A nested models test was not followed because the aim of this research was to propose success factors rather than to identify the most parsimonious model.

7.7.1 Content validity

Prior to launching the survey, the questionnaire was pilot-tested to validate content validity and was generated first in an English version and then in Thai. The process for pilot testing described at this point in Chapter 3, p.68. Two researchers were engaged to validate the items to ensure that sense and meaning were clearly represented. Ten

experts (senior management staff from a sample who have performed ICT risk management in their organisations) were engaged to confirm understanding of each question in the questionnaire. These experts only changed the contents where the clarity of meaning needed improvement. For example, question number 50 asked to what extent a respondent agreed with the statement: "The organisation manages several types of operating software in order to generate data and information in the same file pattern". The experts recommended that the researcher should provide an example to elucidate the meaning of "same file pattern" to make this statement clearer. Therefore, the researcher added types of operation system (Oracle, UNIX and SAP): For example, "the data and information were treated using SAP software, and must not be treated using other software" (repeated in Chapter 3, p. 68). After making these final changes of a survey question, ten surveys amended by the ten experts were included in the survey.

7.7.2 Construct validity

Construct validity or dimension validity was used to confirm that the indicators aligned with the factors as they are measuring instrument adequacy (Schwab 1980; O'Leary-Kelly & Vokurka 1998; Cronbach & Meehl 1955). Dimension validity is based on the tests of convergent validity, discriminant validity and nomological validity.

7.7.3 Convergent validity

In SEM, the researcher is able to use CFA to estimate the values of factor loading between the indicators and the factor. The factor loadings indicate the correlation between the indicators and the factor. CFA allows the researcher to consider the item reliability by looking at squared multiple correlations. The factor loading should exceed .70 and the squared multiple correlations should be greater than .50 for each indicator in the factor (Hair et al. 2006). In this research, if the indicators within the factor did not meet these requirements, they were deleted from the factor to ensure the accuracy of information on the factor. Moreover, modification indices were also used in the early stage of validity testing, in line with Holmes-Smith's (2007 p. 6-3) suggestion that 'For a one-factor congeneric measurement model to be accepted as a good fitting model, the indicator variables contributing to the overall measurement of the latent variable must all be of the same kind. That is, they must all represent the same generic true score—they must all be valid measures of the one latent trait'. Thus, this research used CFA in a one-factor congeneric measurement model as part of the structural model to test item reliability (Jöreskog & Sörbom 1989). CFA began with the evaluation of each dimension

or construct, as outlined in the next section. The next section also discusses the model assessment and modification.

7.8 Stage V: Confirmatory factor analysis (CFA)

Maximum likelihood (ML) and bootstrapping were used in conjunction with CFA in this research (Kaplan 2000; Olsson et al. 2000). Because ML is an estimator, it provides the most reliable estimation technique in SEM when dealing with a small sample size (Kaplan 2000; Olsson et al. 2000). ML is also good for dealing with multivariate normal distribution. To test multivariate normal distribution, Mardia's coefficient was calculated and the results were shown in AMOS. Mardia's coefficient measures multivariate kurtosis and the critical ratio of all items in multivariate analyses (Mardia, 1970). For example, based on the results generated by AMOS, Mardia's coefficient value was 32.070 and its critical ratio was 40.222 for the POLICY factor (see Table 7-17). The critical ratio value indicates that the data in this survey do not follow a multivariate normal distribution, thereby being greater than 1.96 (Mardia 1970). Thus, ML would lead to inaccurate results in SEM (Olsson 1979).

To deal with inaccurate results, the bootstrapping technique was selected to boost the accuracy of values. Because this resampling technique allows the researcher to test the model under conditions of multivariate normal distribution accurate results can be obtained (Byrne 2001). Moreover, bootstrapping allows the researcher to resample the data from a large sample size as new data based on the actual data of this research. In particular, it not only simulates the data as if it was real but also calculates the p-value with a Bollen-Stine bootstrap used in this research to test the significance for obtaining the χ^2 value (Bollen 1989). In this regard, the results of the p-value from the Bollen-Stine bootstrap and from the actual data should exceed .05 to be accepted for model fit.

To conduct model assessment of the structural model it is necessary to use goodness of fit (GOF) tests. GOF is a set of measure indices that indicate the accuracy of a model in explaining the data. There are several GOF measures for assessing a structural model but it is not recommended to report on them all (Jaccard & Wan 1996; Kline 1998). Thus, certain GOF measures were selected to assess the model fit in this research, which are discussed in the following paragraph.

Absolute fit indices and incremental fit indices were used for GOF measures (Tabachnick & Fidell 2007) in this research (refer to Chapter 3, p. 71 for further information). Accordingly, the structural model is used to evaluate how well the model can explain the data gathered from the qualitative analysis. According to Hair et al. (2006), at least one

GOF measure from each type of measure should be selected. Jaccard and Wan (1996) suggest that at least three GOF measures be selected for the model assessment. While Kline (1998) recommends that at least four GOF measures be selected, this research uses seven GOF measures[5] selected from both absolute fit and incremental fit indices to assess the model fit based upon χ^2/df or normed chi-square, the p-value, the Comparative Fit Index (CFI), the Tucker-Lewis Index (TLI), the standardised root mean square residual (SRMR), the root mean square error of approximation (RMSEA), and HOELTER's critical N (HOELTER) as the requirements. If all GOF measurement requirements are not met, model modifications are necessary to ensure the model can adequately explain the data.

The researcher set up four processes for rectifying the model, and set up guidelines for model modification to ensure any changes were carefully undertaken. Thus, each step was carefully applied to reduce the potential for errors in the model (Byrne 2001; Hair et al. 2006), as per the following:

- Factor loadings are values that indicate how an item can accurately explain a factor. The factor loadings of indicators should be greater than 0.7, otherwise they will be dropped because they cannot sufficiently explain the factors (Hair et al. 2006).
- The p-value of each observed variable is the value that represents the significance of an item in the model. P>.05 for an observed variable means that it is not significant, and that it will be deleted excepting unreliable items from the model.
- Modification indices (MI) are values representing the highest covariance values, which suggest that the particular indicator relates to misspecification (Byrne 2001; Hair et al. 2006) between two variables as illustrated in the list of MI (e.g. in Table 7-15), and such values will be subject to deletion after careful consideration. Thus, the factor loadings will be used together with MI

[5] According to Garson's statnotes (2009),

Normed chi-square refers to the model chi-square which 'is a badness of fit measure in that a finding of significance means the given model's covariance structure is significantly different from the observed covariance matrix. If model chi-square <.05 [*P-value*], the researcher's model is rejected by this criterion' (Garson 2009, p. 23).

CFI is to 'compare the existing model fit with a null model which assumes the indicator variables (and hence also the latent variables) in the model are uncorrelated (the "independence model")' (Garson 2009, p. 29).

TLI is one of the fit indexes less affected by sample size. 'To make comparisons between factor models, chi-squares were compared, with significant reductions in the chi-square indicating a better fit of the data than the theoretical model' (Gordon 2001, p. 1).

SRMR is 'the average difference between the predicted and observed variances and covariances in the model, based on standardised residuals' (Garson 2009, p. 25).

RMSEA is the best way to check for the fit of the model because chi-square value based fit indices are influenced largely by the sample size and the number of parameters in the model (Garson 2009).

HOELTER's critical N is 'issued to judge whether or not sample size is adequate' (Garson 2009, p. 25).

values to justify which particular indicator will be discarded. Having lower factor loadings between two variables means they will be deleted. After dropping one, the researcher will run the analysis again to measure the factor loadings for all indicators and the MI. The process will be repeated until there is no significant value.

- GOF cut-of-values were set at χ^2/df<3 and p>.05 (Carmines & McIver 1981; Ullman 2001), CFI≥.95 (Carlson & Mulaik 1993), TLI≥.95 (Hu & Bentler 1998), SRMR<.08 (Byrne 1994, 2001; Hair et al. 2006), RMSEA<.06 (Yu 2002), HOELTER≥200 (Hoelter 1983) and CR>1.96 (Mardia 1970), which represent a good model fit and that the model can adequately explain the survey data when the requirements for all of these indices have been met (see Table 7-16).

Table 7-16: Measurement indices guidelines adapted for this research

GOF Test	Name	Cut-off Value	References
χ^2/df	Normed Chi-square	< 3	Carmines & Mclver (1981) Ullman (2001)
p	Probability value	> .05	
CFI	Comparative fit index	≥ .95	Carlson & Mulaik (1993)
TLI	Tucker-Lewis index	≥ .95	Hu & Bentler (1998)
SRMR	Standardised root mean square residual	< .08	Byrne (1994, 2001) Hair et al. (2006)
RMSEA	Root mean square error of approximation	< .06	Yu (2002)
HOELTER	Hoelter's critical N (at a confidence level of 95%)	≥ 200	Hoelter (1983)
CR	Critical Ratio If it exceeds 1.96, the bootstrapping technique can be undertaken.	>1.96	Mardia (1970)

The model modification process in this research followed the processes and guidelines listed above. The model modification was applied through the convergent, discriminant, nomological, measurement and structural model validities when the model did not fit with the data. An analysis of the application of these processes to each factor follows.

7.8.1 Organisational policy (POLICY)

As shown in Figure 7-6, the factor loadings (λ) of all indicators in POLICY are greater than .70 and the squared multiple correlations (R^2) of all indicators exceed .50. This means that all indicators represent a good fit for POLICY.

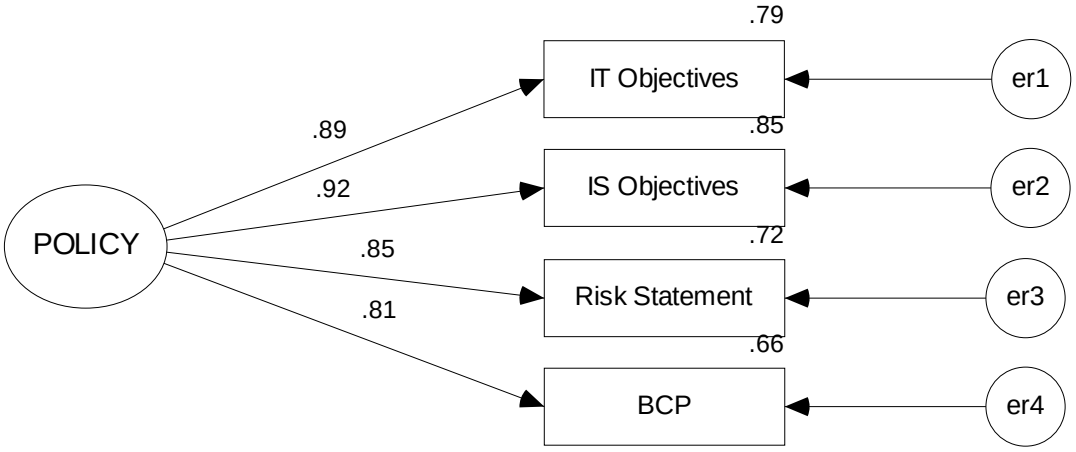


Figure 7-6: POLICY congeneric measurement model

However, the initial output values of the POLICY dimension as a one-dimension congeneric measurement model revealed that the model did not meet the cut-off value requirements regarding GOF indices: χ^2/df (13.749/2)=6.874, p=.076, TLI=.963, CFI=.988, RMSEA=.140, SRMR=.018, and HOELTER=132 with a confidence level of 95%, as shown in Table 7-17.

Table 7-17: POLICY congeneric measurement model with indices

Indicator		Factor	Standardised Regression Weights (λ)		Squared Multiple Correlations (R^2)		Model Fit			Cut-off Value Requirement
			Before	After	Before	After	Indices	Before	After	
Policy1	<---	POLICY	.878	.892	.771	.796	χ^2/df	6.874	.688	<3
Policy2	<---	POLICY	.913	.936	.833	.876	P-value	.076	.461	>.05
Policy3	<---	POLICY	.854	.830	.730	.688	TLI	.963	1.002	≥.95
Policy4	<---	POLICY	.812	.788	.659	.622	CFI	.988	1.000	≥.95
							RMSEA	.140	.000	<.06
							SRMR	.018	.003	<.08
							HOELTER P=0.05	132	1680	≥200
							Multivariate normal distribution test			
							Kurtosis	32.070	32.070	
							Critical ratio of kurtosis	40.222	40.222	>1.96

Therefore, this initial model was rejected and model modifications were applied. Only MIs were considered to modify the model because the squared multiple correlations of all indicators were met and all indicators were found to be significant (see Table 7-18). MI suggested that there was covariance between er3 and er4.

Table 7-18: The p-value of each indicator and modification indices in covariance

				Estimate	S.E.	C.R.	P
policy1	<---		POLICY	1.062	.055	19.381	***
policy2	<---		POLICY	1.104	.053	20.703	***
policy3	<---		POLICY	1.159	.064	18.024	***
policy4	<---		POLICY	1.014	.060	16.809	***
			M.I.	Par Change			
er3	<-->	er4	10.678	.115			

Figure 7-7 shows the POLICY congeneric model modification that was then generated in order to rectify the model fit. This revealed that the model was a good fit with the new values of χ^2/df (.688/1) = .688, p= .461, TLI= 1.002, CFI= 1.000, RMSEA= .000, SRMR= .003, and HOELTER=1680 with a confidence level of 95%, as shown in Table 7-17.

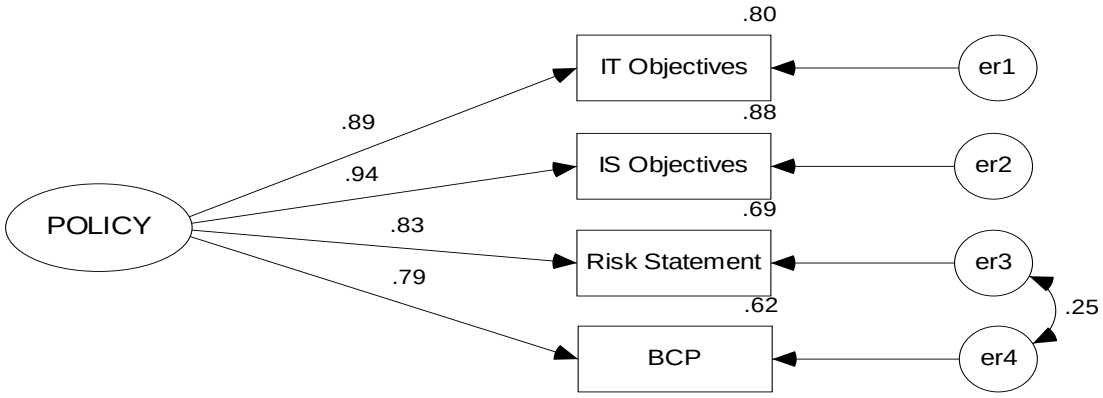


Figure 7-7: POLICY congeneric measurement model modifications

Having a χ^2/df value of .688 and a p-value of .461 indicates that this model fits well, but the squared multiple correlations suggest that although the dimension POLICY explained over 62% of the variance in four indicator variables, the covariance term between er3 and er4 (see Figure 7-7) suggests that there is a correlation between policy[6] (risk statement) and policy4 (business continuity plan) that was not explained by POLICY alone[7]. However, the variance in policy3 and policy4 then represented that both

[6] Small letter represents the indicators in each dimension.
[7] Capital letter represents the dimension.

indicators were explained by over 62% in POLICY. Thus, the POLICY dimension was accepted to be a latent variable in the structural model.

7.8.2 Human resource management and planning (HRMP)

As shown in Figure 7-8, the factor loadings of all indicators in HRMP are greater than .70 and the squared multiple correlations of all indicators exceed .50. This means that all indicators represented a good fit for HRMP.

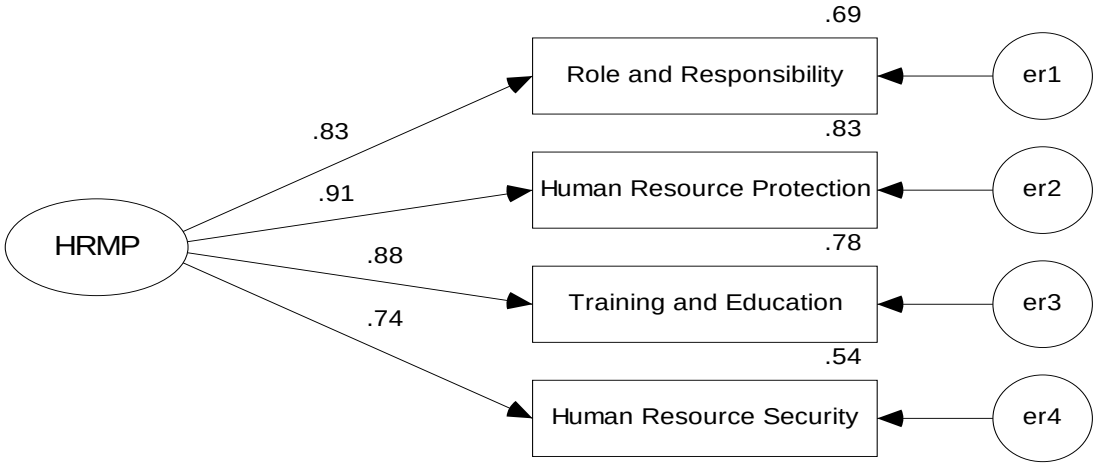


Figure 7-8: HRMP congeneric measurement model

However, the initial output values of the HRMP dimension revealed that the model was not fitted with the requirements regarding GOF indices: χ^2/df (8.777/2)=4.389, p=.114, TLI=.975, CFI=.992, RMSEA=.106, SRMR=.017, and HOELTER=206 with a confidence level of 95%, as shown in Table 7-19.

Table 7-19: HRMP congeneric measurement model with indices

Indicator		Factor	λ		R^2		Model Fit			Cut-off value Requirement
			Before	After	Before	After	Indices	Before	After	
hrmp1	<---	HRMP	.831	.836	.691	.698	χ^2/df	4.389	.000	<3
hrmp2	<---	HRMP	.908	.924	.825	.855	P-value	.114	.990	>.05
hrmp3	<---	HRMP	.884	.863	.781	.745	TLI	.975	1.007	≥.95
hrmp4	<---	HRMP	.737	.706	.544	.498	CFI	.992	1.000	≥.95
							RMSEA	.106	.000	<.06
							SRMR	.017	.000	<.08
							HOELTER P=0.05	206	2774030	≥200
							Multivariate normal distribution test			
							Kurtosis	29.614	29.614	
							Critical ratio of kurtosis	37.141	37.141	>1.96

Therefore, this initial model was rejected and model modifications were applied. Only MIs were considered to modify the model because the squared multiple correlations of all indicators were met and all indicators were significant (see Table 7-20). MI suggested that there was covariance between er3 and er4.

Table 7-20: The p-value of each indicator and modification indices in covariance

			Estimate	S.E.	C.R.	P
hrmp1	<---	HRMP	1.000			
hrmp2	<---	HRMP	.997	.051	19.484	***
hrmp3	<---	HRMP	.978	.052	18.836	***
hrmp4	<---	HRMP	.717	.050	14.466	***
			M.I.	Par Change		
er3	<-->	er4	6.280	.073		

Figure 7-9 demonstrates the HRMP congeneric measurement model modification that was then generated in order to rectify the model fit. This model was seen to be a good fit with the new values of χ^2/df(.000/1)=.000, p=.990, TLI=1.007, CFI=1.000, RMSEA=.000, SRMR=.001, and HOELTER=2774030 with a confidence level of 95%, as shown in Table 7-19.

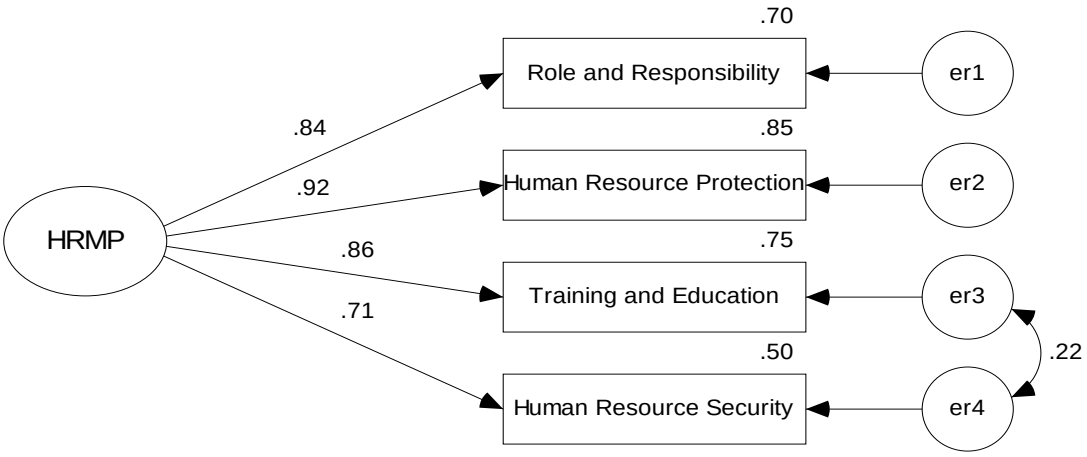


Figure 7-9: HRMP congeneric measurement model modifications

With a χ^2/df value of .000 and a p-value of .990, this model fits well, but the squared multiple correlations suggest that although the dimension HRMP explains over 50% of the variance in four indicator variables, the covariance term between er3 and er4 indicates (see Figure 7-9) that there is a correlation between hrmp3 (training and education) and hrmp4 (human resources security) that is not explained by HRMP alone. However, the variance in hrmp3 and hrmp4 is explained by over 50% in HRMP. Thus, the HRMP dimension was accepted as a latent variable in the structural model.

7.8.3 Organisational information security (OS)

As summarised in Figure 7-10, the factor loadings for all indicators in OS are greater than .70 and the squared multiple correlations of all indicators exceed .50, excepting os6 (physical protection), which was therefore dropped. Moreover, os1 (system configuration) was discarded as it was duplicated with it1 and it2 (networking and personal computers respectively) in the IT dimension (see p. 191). The remaining indicators were accepted as a good fit for OS.

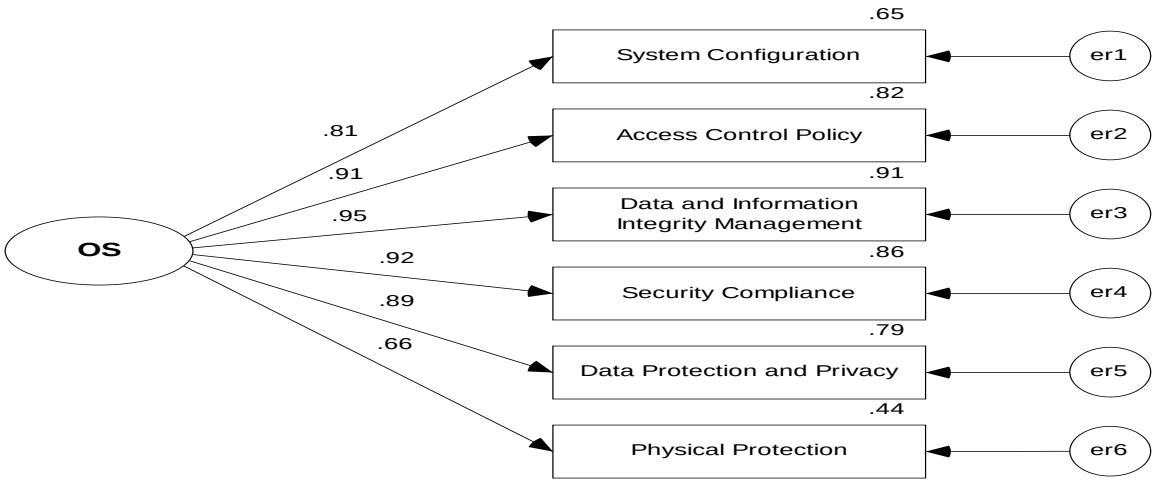


Figure 7-10: OS congeneric measurement model

However, the initial output values of the OS dimension revealed that the model was not fitted with the requirements regarding GOF indices: χ^2/df (40.123/9)=4.458, p=.030, TLI=.971, CFI=.983, RMSEA=.003, SRMR=.023, and HOELTER=127 with a confidence level of 95%, as shown in Table 7-21.

Table 7-21: OS congeneric measurement model with indices

Indicator		Factor	λ		R^2		Model Fit			Cut-off value Requirement
			Before	After	Before	After	Indices	Before	After	
os1	<---	OS	.803	-	.645	-	χ^2/df	4.458	.030	<3
os2	<---	OS	.907	.914	.815	.835	P-value	.030	.904	>.05
os3	<---	OS	.951	.943	.908	.890	TLI	.971	1.004	≥.95
os4	<---	OS	.925	.944	.862	.891	CFI	.983	1.000	≥.95
os5	<---	OS	.888	.888	.788	.788	RMSEA	.003	.000	<.06
os6	<---	OS	.663	-	.440	-	SRMR	.023	.001	<.08
							HOELTER P=0.05	127	38997	≥200
							Multivariate normal distribution test			
							Kurtosis	40.432	22.010	
							Critical ratio of kurtosis	35.856	27.604	>1.96

Not all of the requirements of these indices were met, which led to this initial model being rejected and model modifications being applied. Only MIs were considered to modify the model because the squared multiple correlations of all indicators were met and all indicators were significant (Table 7-22). MI suggested that there was covariance between er2 and er4.

Table 7-22: The p-value of each indicator and modification indices in covariance

			Estimate	S.E.	C.R.	P
os2	<---	OS	.904	.045	19.938	***
os3	<---	OS	.991	.045	22.243	***
os4	<---	OS	1.046	.049	21.200	***
os5	<---	OS	1.090	.055	19.700	***
			M.I.	Par Change		
er2	<-->	er4	5.531	-.031		

Figure 7-11 shows the OS congeneric measurement model modification that was then generated in order to rectify the model fit. This indicated that the model was a good fit with the new values of χ^2/df (.030/1)=.030, p=.904, TLI=1.004, CFI=1.000, RMSEA=.000, SRMR=.001, and HOELTER=38997 with a confidence level of 95%, as shown in Table 7-21.

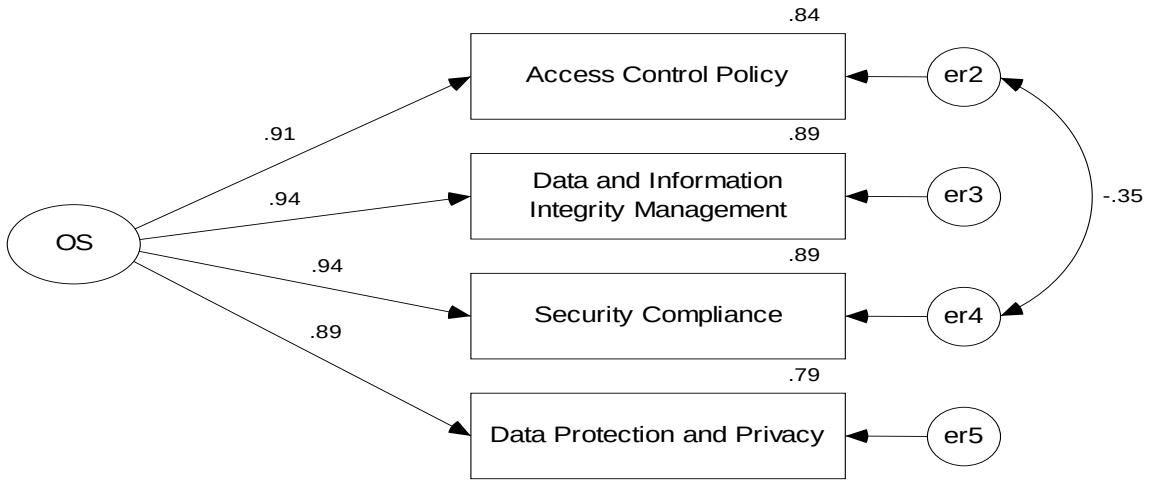


Figure 7-11: OS congeneric measurement model modifications

With a χ^2/df value of .030 and a p-value of .904 this model fits well, but the squared multiple correlations suggest that although the dimension OS explains over 79% of the variance in four indicator variables, the covariance term between er2 and er4 (see Figure 7-11) implies that there is a correlation between os2 (access control policy) and os4 (security compliance) that is not explained by OS alone. However, the variance in policy2 and policy4 shows that both indicators were explained by over 84% in OS. As a result, the OS dimension was accepted as a latent variable in the structural model.

7.8.4 Management of ICT resources (IT)

As outlined in Figure 7-12, the factor loadings of all indicators in IT are greater than .70 and the squared multiple correlations of all indicators exceed .50. This means that all indicators were accepted as a good fit for IT.

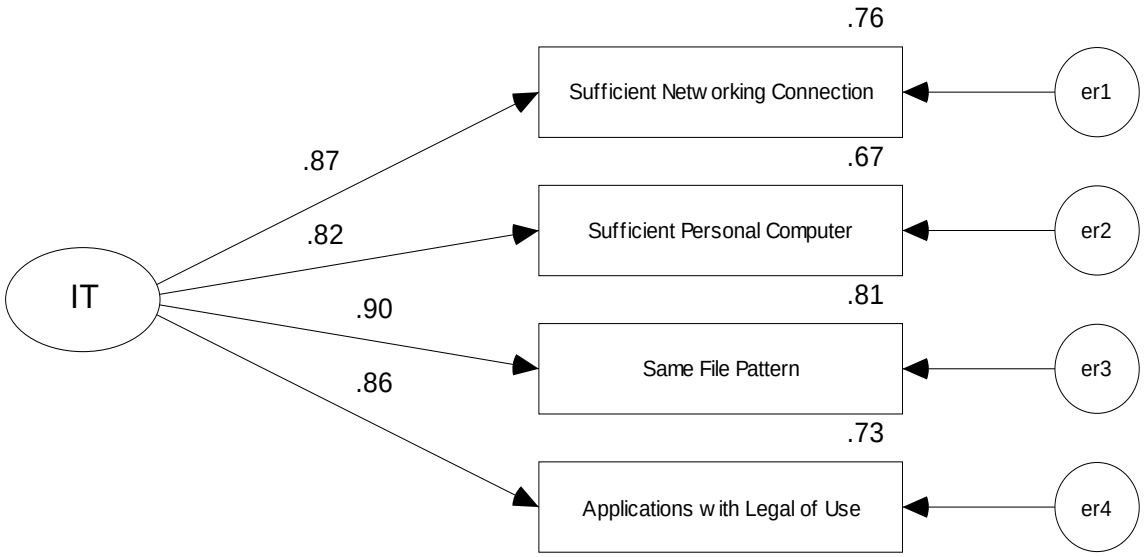


Figure 7-12: IT congeneric measurement model

However, the initial output values of the IT dimension did not meet the requirements regarding GOF indices: χ^2/df (61.404/2)=30.702, p=.002, TLI=.809, CFI=.936, RMSEA=.314, SRMR=.039, and HOELTER=30 with a confidence level of 95%, as shown in Table 7-23.

Table 7-23: IT congeneric measurement model with indices

Indicator		Factor	λ		R^2		Model Fit			Cut-off value Requirement
			Before	After	Before	After	Indices	Before	After	
it1	<---	IT	.870	.810	.757	.657	χ^2/df	30.702	.303	<3
it2	<---	IT	.818	.745	.669	.556	P-value	.002	.782	>.05
it3	<---	IT	.899	.939	.802	.882	TLI	.809	1.004	≥.95
it4	<---	IT	.855	.874	.732	.764	CFI	.936	1.000	≥.95
							RMSEA	.314	.000	<.06
							SRMR	.039	.002	<.08
							HOELTER P=0.05	30	3820	≥200
							Multivariate normal distribution test			
							Kurtosis	40.746	40.746	
							Critical ratio of kurtosis	51.102	51.102	>1.96

Consequently, this initial model was rejected and model modifications were applied. Only MIs were considered to modify the model because the squared multiple correlations of all indicators were met and all indicators were significant (see Table 7-24). MI suggested that there was covariance between er1 and er2.

Table 7-24: The p-value of each indicator and modification indices in covariance

			Estimate	S.E.	C.R.	P
it1	<---	IT	1.000			
it2	<---	IT	.993	.055	17.984	***
it3	<---	IT	.950	.045	21.129	***
it4	<---	IT	.904	.047	19.429	***
			M.I.	Par Change		
er1	<-->	er2	42.348	.187		

Figure 7-13 shows the IT congeneric measurement model modification that was generated in order to rectify the model fit. It was demonstrated that this model was a good fit with the new values of χ^2/df(.303/1)=.303, p=.782, TLI=1.004, CFI=1.000, RMSEA=.000, SRMR=.002, and HOELTER=3820 with a confidence level of 95%, as shown in Table 7-23.

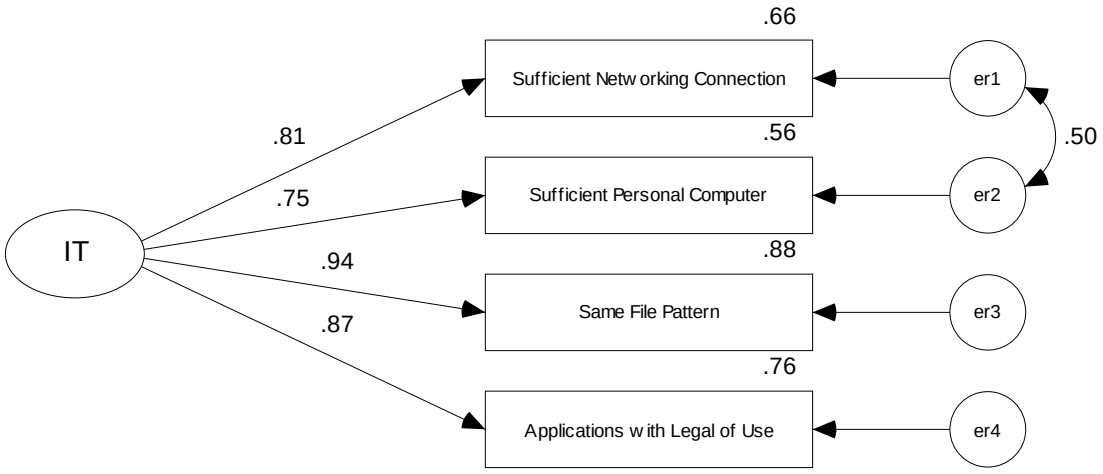


Figure 7-13: IT congeneric measurement model modifications

With a χ^2/df value of .303 and a p-value of .782, this model fits well, but the squared multiple correlations suggest that although the dimension IT explains over 56% of the variance in the four indicator variables, the covariance term between er1 and er2 (see Figure 7-13) indicates that there is a correlation between it1 (sufficient networking connection) and it2 (sufficient personal computers) that is not explained by IT alone. However, the variance in it1 and it2 revealed that both indicators were explained by over 56% in IT. As a result, the IT dimension was accepted as a latent variable in the structural model.

7.8.5 The corporate level plan (CLP)

As shown in Figure 7-14, the factor loadings of all indicators in CLP are greater than .70 and the squared multiple correlations of all indicators exceed .50. This means that all indicators were accepted as a good fit for CLP.

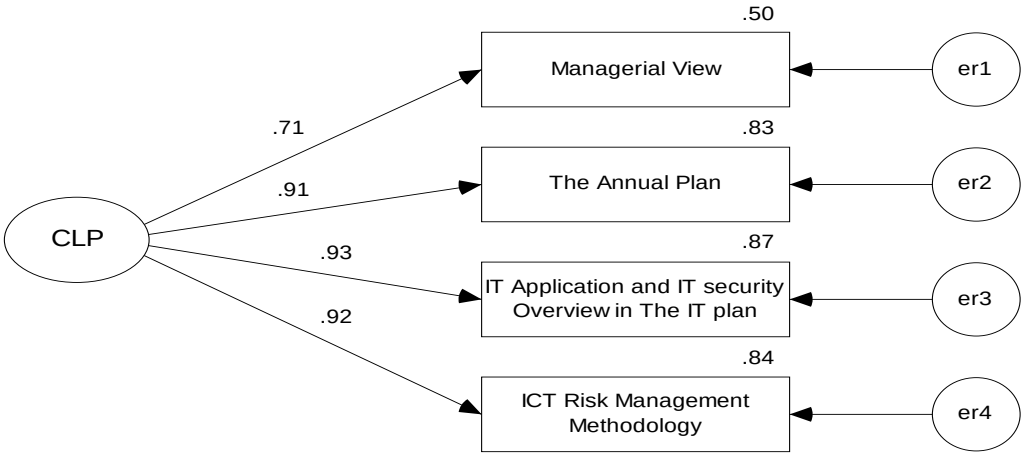


Figure 7-14: CLP congeneric measurement model

However, the initial output values of the CLP dimension revealed that the model did not fit the requirements regarding GOF indices: χ^2/df(5.747/2)=2.873, p=.503, TLI=.989, CFI=.996, RMSEA=.079, SRMR=.012, and HOELTER=314 with a confidence level of 95%, as shown in Table 7-25.

Table 7-25: CLP congeneric measurement model with indices

Indicator		Factor	λ		R^2		Model Fit			Cut-off value Requirement
			Before	After	Before	After	Indices	Before	After	
clp1	<---	CLP	.709	.695	.503	.482	χ^2/df	2.873	1.288	<3
clp2	<---	CLP	.908	.902	.825	.814	P-value	.503	.609	>.05
clp3	<---	CLP	.933	.936	.870	.875	TLI	.989	.998	≥.95
clp4	<---	CLP	.917	.920	.840	.846	CFI	.996	1.000	≥.95
							RMSEA	.079	.031	<.06
							SRMR	.012	.005	<.08
							HOELTER P=0.05	314	898	≥200
							Multivariate normal distribution test			
							Kurtosis	33.045	33.045	
							Critical ratio of kurtosis	41.443	41.443	>1.96

Only the RMSEA index did not meet the requirements. Therefore this initial model was rejected and model modifications were applied. Only MIs were considered to modify the model because the squared multiple correlations of all indicators were met and all

indicators were significant (see Table 7-26). MI suggested that there was covariance between er1 and er2.

Table 7-26: The p-value of each indicator and modification indices in covariance

			Estimate	S.E.	C.R.	P
clp1	<---	CLP	1.000			
clp2	<---	CLP	1.052	.075	13.944	***
clp3	<---	CLP	1.186	.078	15.272	***
clp4	<---	CLP	1.166	.076	15.312	***
			M.I.	Par Change		
er1	<-->	er2	6.449	.096		

Figure 7-15 depicts the CLP congeneric measurement model modification that was generated in order to make the model fit. This demonstrated that the model was a good fit with the new values of χ^2/df(1.288/1)=1.288, p=.609, TLI=.998, CFI=1.000, RMSEA=.031, SRMR=.005, and HOELTER=898 with a confidence level of 95%, as shown in Table 7-25.

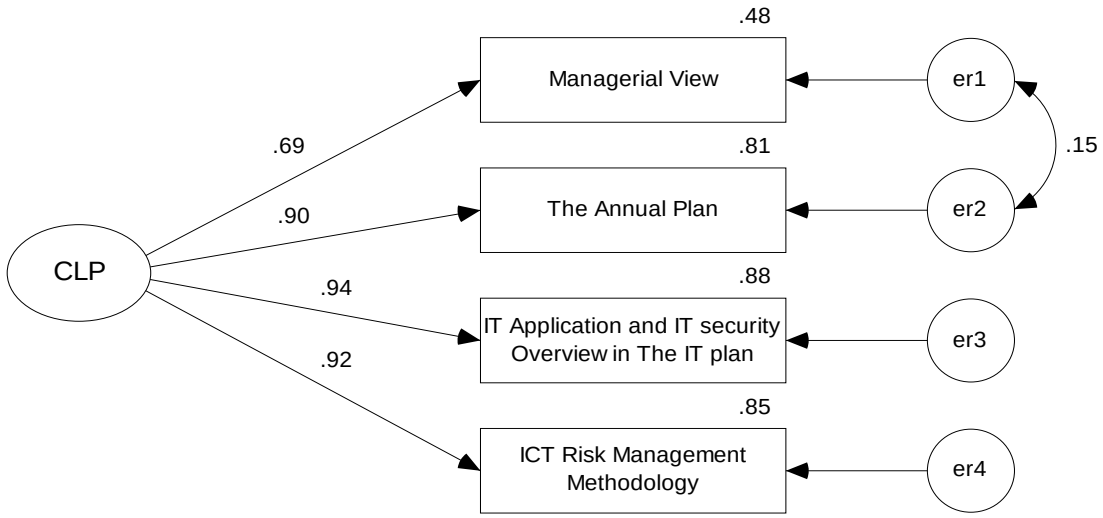


Figure 7-15: CLP congeneric measurement model modifications

With a χ^2/df value of 1.288 and a p-value of .609 this model fits well, but the squared multiple correlations suggest that although the dimension CLP explained over 48% of the variance in four indicator variables, the covariance term between er1 and er2 (see Figure 7-15) implies that there is a correlation between clp1 (managerial view as top-down approach) and clp2 (the corporate plan) that is not explained by CLP alone. However, the variance in clp1 and clp2 revealed that both indicators were explained by over 48% in CLP. As a result, the CLP dimension was accepted as a latent variable in the structural model.

7.8.6 The operational level plan (OLP)

As shown in Figure 7-16, the factor loadings of three indicators are greater than .70 and the squared multiple correlations of three indicators exceed .50, but the olp1 (operational view as bottom-up approach) indicator was lower than .70 and .50 in these measures respectively.

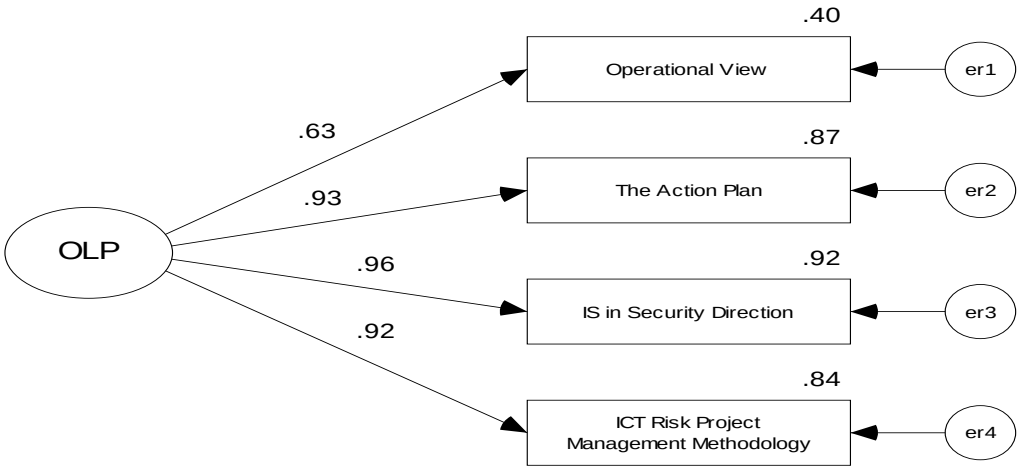


Figure 7-16: OLP congeneric measurement model

All indicators were significant (see Table 7-27). Moreover, the MIs did not suggest a need to rectify the model, thereby having no covariance among indicators.

Table 7-27: The p-value of each indicator and modification indices in covariance

			Estimate	S.E.	C.R.	P
olp1	<---	OLP	1.000			
olp2	<---	OLP	1.326	.101	13.114	***
olp3	<---	OLP	1.481	.111	13.370	***
olp4	<---	OLP	1.380	.106	12.980	***
			M.I.	Par Change		
-	-	-	-	-		

The output values of the OLP dimension revealed that the model fitted well with the requirements regarding GOF indices: χ^2/df (3.406/2)=1.703, p=.353, TLI=.996, CFI=.999, RMSEA=.048, SRMR=.010, and HOELTER=530 with a confidence level of 95%, as shown in Table 7-28.

Table 7-28: OLP congeneric measurement model with indices

Indicator		Factor	λ	R^2	Model Fit		Cut-off value Requirement
					Indices	Cut-off Value	
olp1	<---	OLP	.630	.397	χ^2/df	1.703	<3
olp2	<---	OLP	.930	.866	P-value	.353	>.05
olp3	<---	OLP	.961	.924	TLI	.996	≥.95
olp4	<---	OLP	.916	.839	CFI	.999	≥.95
					RMSEA	.048	<.06
					SRMR	.010	<.08
					HOELTER P=0.05	530	≥200
					Multivariate normal distribution test		
					Kurtosis	23.869	
					Critical ratio of kurtosis	29.935	>1.96

Although olp1 (operational view as bottom-up approach) is a less reliable measure of OLP, it did not affect the model fit. As a result, the OLP dimension was accepted as a latent variable in the structural model with a greater value of indices.

7.8.7 Successful ICT risk management (SICTRM)

As outlined in Figure 7-17, the number of parameters to be estimated is equal to the number of sample moments; this then leads to the model being 'just-identified' (Byrne 2001). As a result, this model was fixed with constraint to be 'over-identified' in order to estimate the value of indices (Byrne 2001).

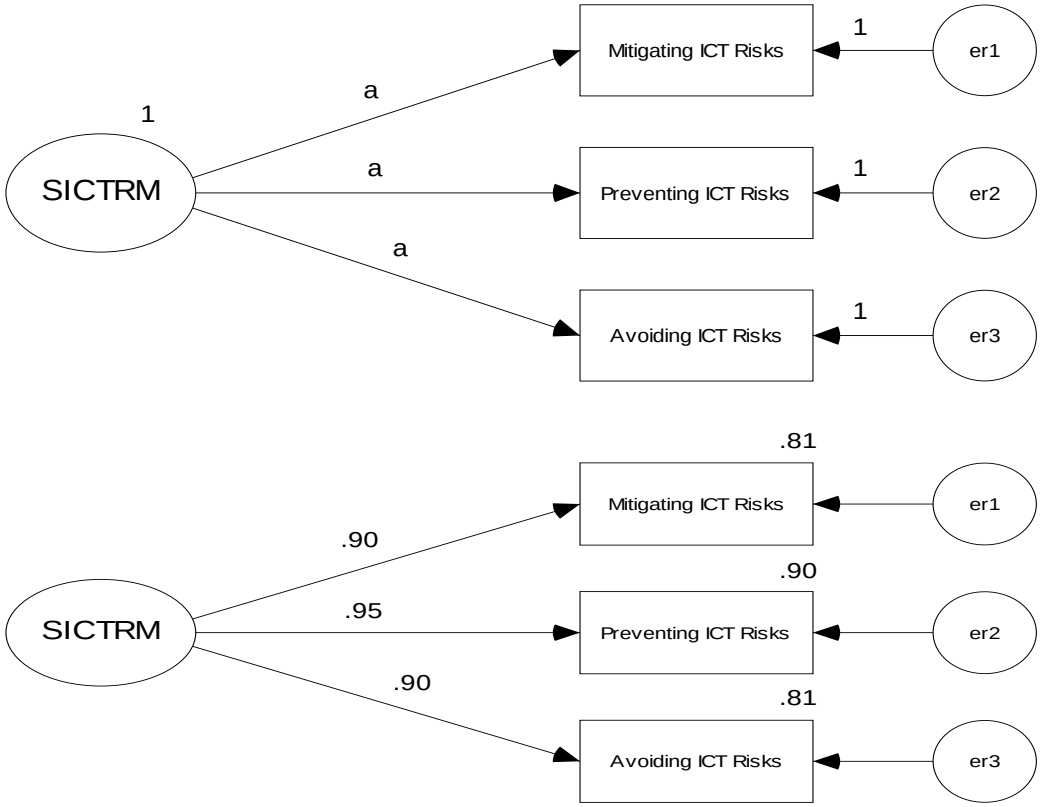


Figure 7-17: SICTRM congeneric measurement model

The values of indices were as follows: χ^2/df =3.716, TLI=.990, CFI=.993, RMSEA=.095, SRMR=.008, p=.146 and HOELTER=243 with a confidence level of 95%, as shown in Table 7-29.

Table 7-29: SICTRM congeneric measurement model with indices

Indicator		Factor	λ		R^2		Model Fit			Cut-off value Requirement
			Before	After	Before	After	Indices	Before	After	
sictrm1	<---	SICTRM	.916	.897	.840	.805	χ^2/df	-	3.716	<3
sictrm2	<---	SICTRM	.943	.948	.890	.899	P-value	-	.146	>.05
sictrm3	<---	SICTRM	.891	.899	.793	.809	TLI	-	.990	≥.95
							CFI	1.000	.993	≥.95
							RMSEA	.949	.095	<.06
							SRMR	-	.008	<.08
							HOELTER P=0.05	-	243	≥200
							Multivariate normal distribution test			
							Kurtosis	19.143	19.143	
							Critical ratio of kurtosis	30.368	30.368	>1.96

Although all of these indices did not meet the goodness of fit (GOF), the model can be accepted as a fitted model because the factor loadings for all indicators are greater than

.70 and the squared multiple correlations of all indicators exceed .50. All indicators were significant (see Table 7-30). Moreover, this model was fixed to only estimate the value indices to explain the data in the model; thus, all indicators were accepted as a good fit for SICTRM and this model was accepted.

Table 7-30: The p-value of each indicator and modification indices in covariance

			Estimate	S.E.	C.R.	P
sictrm1	<---	SICTRM	.928	.040	23.157	***
sictrm2	<---	SICTRM	.928	.040	23.157	***
sictrm3	<---	SICTRM	.928	.040	23.157	***

After evaluating convergent validity, all indicators were correlated to their own dimensions, as shown in Table 7-31.

Table 7-31: Summary of factor loadings and squared multiple correlations

Indicator		λ	R^2	Dimension	Indicator		λ	R^2	Dimension
policy1	<---	.892	.796	Organisational Policy (POLICY)	clp1	<---	.695	.482	The Corporate Level Plan (CLP)
policy2	<---	.936	.876		clp2	<---	.902	.814	
policy3	<---	.830	.688		clp3	<---	.936	.875	
policy4	<---	.788	.622		clp4	<---	.920	.846	
hrmp1	<---	.836	.698	Human resource management and Planning (HRMP)	olp1	<---	.630	.397	The Operational Level Plan (OLP)
hrmp2	<---	.924	.855		olp2	<---	.930	.866	
hrmp3	<---	.863	.745		olp3	<---	.961	.924	
hrmp4	<---	.706	.498		olp4	<---	.916	.839	
os2	<---	.914	.835	Organisational Information Security (OS)	sictrm1	<---	.897	.805	Successful ICT Risk Management (SICTRM)
os3	<---	.943	.890		sictrm2	<---	.948	.899	
os4	<---	.944	.891		sictrm3	<---	.899	.809	
os5	<---	.888	.788						
it1	<---	.810	.657	Management of ICT resources (IT)					
it2	<---	.745	.556						
it3	<---	.939	.882						
it4	<---	.874	.764						

It can be concluded that all indicators were found to measure their intended concept (Hair et al. 2006). Therefore, all dimensions were then ready to be evaluated in discriminant validity.

7.9 Stage VI: Discriminant validity

Discriminant validity can be estimated through SEM (Anderson & Gerbing 1988). It should reflect the difference among dimensions in a model. The importance of discriminant validity assessment is in indicating how dimensions in a model are interrelated (Holmes-Smith 2007). If the values of correlations between factors (latent dimensions) exceed .80 (Fornell & Larcker, 1981), .85 (Kline 1998; 2005) or one between .9 and 1.0 (Anderson & Garbing 1988; Hair et al. 2006), this can suggest a lack of discriminant validity. For example, the average variance extracted (AVE) for two dimensions must be greater than the square of the correlation between the dimensions in order to satisfy the requirements of discriminant validity (Holmes-Smith 2007).

In this section, the researcher uses discriminant validity to test among the dimensions in the model that have a correlation of less than .80 (as the requirement in this research) in order to confirm whether those dimensions should represent the data in a different way. However, the modification indices were not used to rectify the model except when the particular dimensions were indifferent. Discriminant validity testing was performed between one dimension and another dimension.

7.9.1 Organisational policy and human resource management and planning (POLICY and HRMP)

As depicted in Figure 7-18, discriminant validity was used to test the correlation between POLICY and HRMP. It was found that the correlation (.76) between POLICY and HRMP was less than .80.

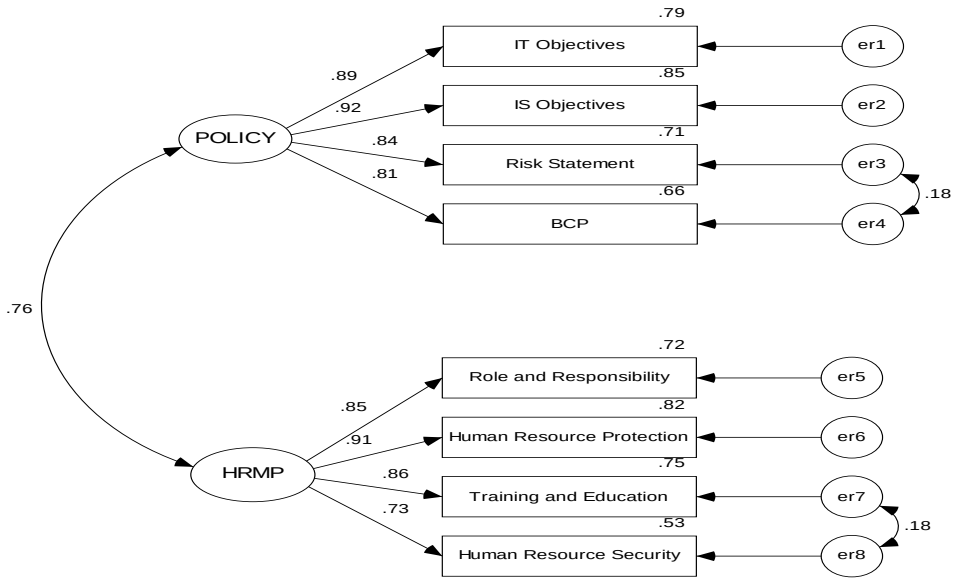


Figure 7-18: Discriminant validity of POLICY and HRMP

According to the assessment of the dimensions, the POLICY dimension was tested with the HRMP dimension to confirm that both dimensions are different from each other.

Table 7-32: POLICY and HRMP for discriminant validity test

POLICY					HRMP					
Indicator	λ	λ^2	ε	AVE	Indicator	λ	λ^2	ε	AVE	ρ^2
policy1	0.888	0.789	0.301		hrmp1	0.849	0.721	0.494		
policy2	0.925	0.856	0.207		hrmp2	0.908	0.824	0.260		
policy3	0.842	0.709	0.543		hrmp3	0.864	0.746	0.378		
policy4	0.810	0.656	0.537		hrmp4	0.727	0.529	0.546		
sum		3.009	1.59	0.655			2.820	1.678	0.627	0.581

The AVE values of POLICY and HRMP are greater than the squared correlation between the dimensions, as shown in Table 7-32. Thus, both the POLICY and HRMP dimensions held discriminant validity.

7.9.2 Organisational policy and organisational information security (POLICY and OS)

As shown in Figure 7-19, discriminant validity was used to test the correlation between POLICY and OS. It was found that the correlation (.78) between POLICY and OS was less than .80.

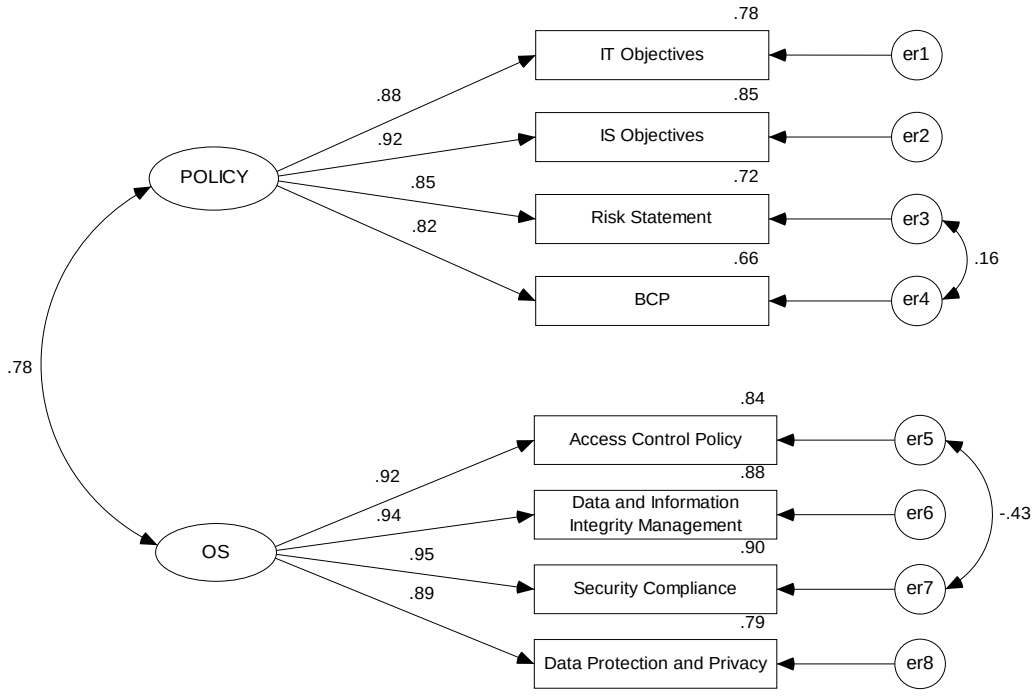


Figure 7-19: Discriminant validity of POLICY and OS

According to the assessment of the dimensions, the POLICY dimension was tested with the OS dimension to confirm that both dimensions are different from each other.

Table 7-33: POLICY and OS for discriminant validity test

POLICY					OS					
Indicator	λ	λ^2	ε	AVE	Indicator	λ	λ^2	ε	AVE	ρ^2
policy1	0.883	0.780	0.314		os2	0.919	0.844	0.158		
policy2	0.922	0.851	0.213		os3	0.940	0.884	0.125		
policy3	0.848	0.719	0.523		os4	0.946	0.895	0.132		
policy4	0.815	0.665	0.524		os5	0.886	0.785	0.322		
sum		3.015	1.574	0.657			3.408	0.737	0.822	0.613

The AVE values of POLICY and OS are greater than the squared correlation between the dimensions, as shown in Table 7-33. Thus, both the POLICY and OS dimensions held discriminant validity.

7.9.3 Organisational policy and management of ICT resources (POLICY and IT)

As shown in Figure 7-20, discriminant validity was used to test the correlation between POLICY and IT. This test found that the correlation (.61) between POLICY and IT was less than .80.

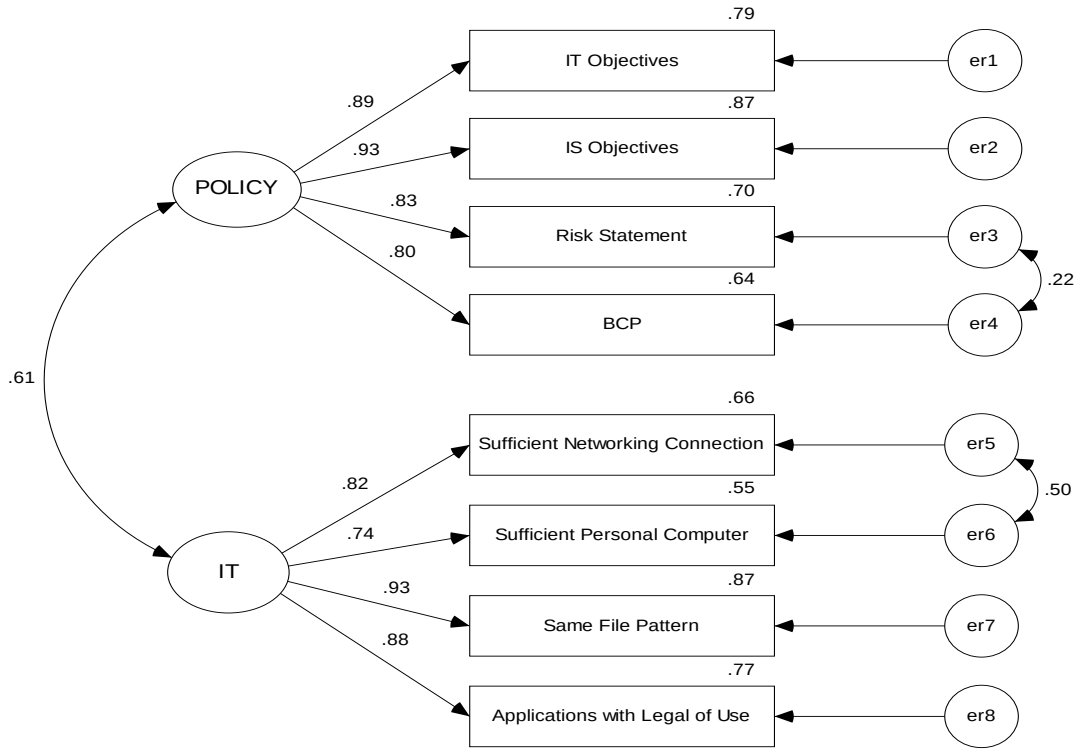


Figure 7-20: Discriminant validity of POLICY and IT

According to the assessment of the dimensions, the POLICY dimension was tested with the OS dimension to confirm that both dimensions are different from each other.

Table 7-34: POLICY and IT for discriminant validity test

POLICY					IT					
Indicator	λ	λ^2	ε	AVE	Indicator	λ	λ^2	ε	AVE	ρ^2
policy1	0.890	0.791	0.298		it1	0.815	0.665	0.460		
policy2	0.932	0.868	0.188		it2	0.742	0.550	0.689		
policy3	0.834	0.696	0.567		it3	0.932	0.869	0.152		
policy4	0.800	0.640	0.562		it4	0.88	0.775	0.262		
sum		2.995	1.615	0.650			2.859	1.563	0.647	0.370

The AVE values of POLICY and OS are greater than the squared correlation between the dimensions, as shown in Table 7-34. Thus, both the POLICY and OS dimensions held discriminant validity.

7.9.4 Organisational policy and the corporate level plan (POLICY and CLP)

As Figure 7-21 depicts, discriminant validity was used to test the correlation between POLICY and CLP. It was found that the correlation (.80) between POLICY and CLP was equal to .80.

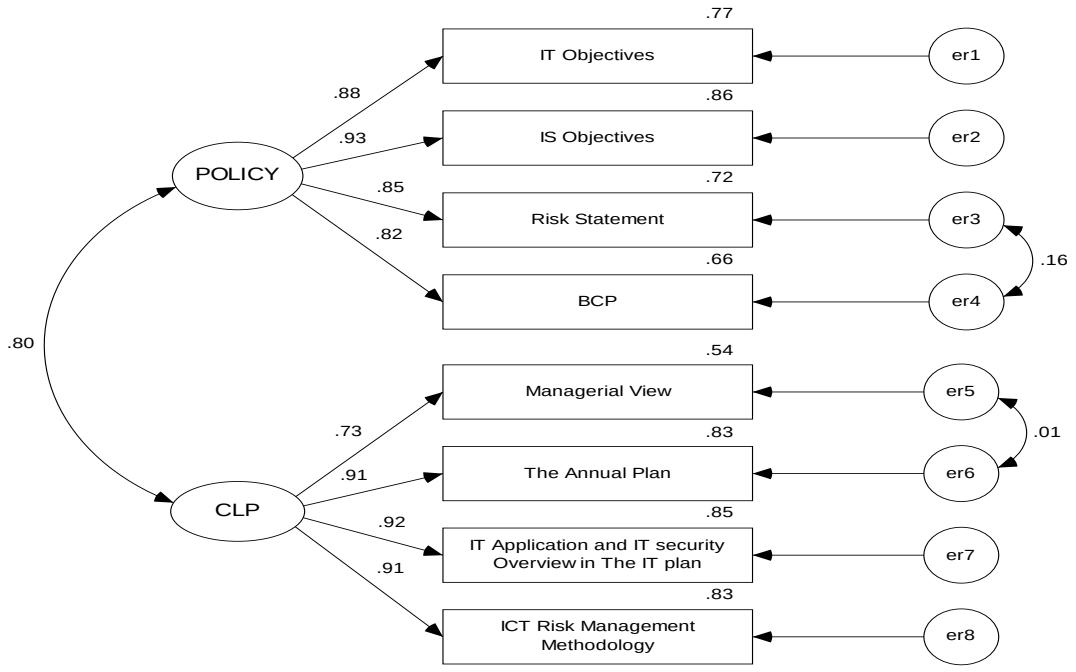


Figure 7-21: Discriminant validity of POLICY and CLP

However, these dimensions still held discriminant validity. According to the assessment of the dimensions, the POLICY dimension was tested with the CLP dimension to confirm that both dimensions are different from each other.

Table 7-35: POLICY and CLP for discriminant validity test

POLICY					CLP					
Indicator	λ	λ^2	ε	AVE	Indicator	λ	λ^2	ε	AVE	ρ^2
policy1	0.877	0.769	0.330		clp1	0.734	0.539	0.792		
policy2	0.928	0.860	0.199		clp2	0.913	0.834	0.204		
policy3	0.848	0.720	0.522		clp3	0.925	0.855	0.205		
policy4	0.815	0.661	0.524		clp4	0.911	0.830	0.231		
sum		3.010	1.575	0.656			3.058	1.432	0.681	0.645

The AVE values of POLICY and CLP are greater than the squared correlation between the dimensions, as shown in Table 7-35. Thus, both the POLICY and CLP dimensions held discriminant validity.

7.9.5 Organisational policy and the operational level plan (POLICY and OLP)

As shown in Figure 7-22, discriminant validity was used to test the correlation between POLICY and OLP. It was found that the correlation (.69) between POLICY and OLP was less than .80.

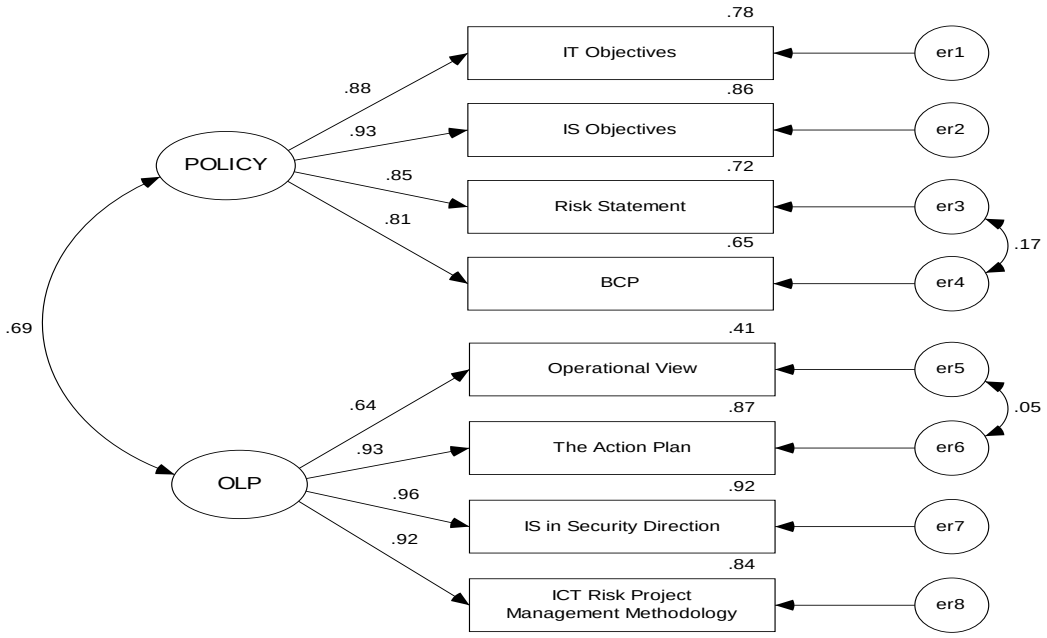


Figure 7-22: Discriminant validity of POLICY and OLP

According to the assessment of the dimensions, the POLICY dimension was tested with the OLP dimension to confirm that both dimensions are different from each other.

Table 7-36: POLICY and OLP for discriminant validity test

POLICY					OLP					
Indicator	λ	λ^2	ε	AVE	Indicator	λ	λ^2	ε	AVE	ρ^2
policy1	0.882	0.778	0.317		olp1	0.637	0.406	1.118		
policy2	0.926	0.857	0.204		olp2	0.934	0.873	0.194		
policy3	0.849	0.722	0.518		olp3	0.957	0.915	0.151		
policy4	0.808	0.653	0.541		olp4	0.916	0.839	0.273		
sum		3.010	1.580	0.656			3.033	1.736	0.636	0.475

The AVE values of POLICY and OLP are greater than the squared correlation between the dimensions, as shown in Table 7-36. Thus, both the POLICY and OLP dimensions held discriminant validity.

7.9.6 Organisational policy and successful ICT risk management (POLICY and SICTRM)

As revealed in Figure 7-23, discriminant validity was used to test the correlation between POLICY and SICTRM. It was found that the correlation (.51) between POLICY and SICTRM was less than .80.

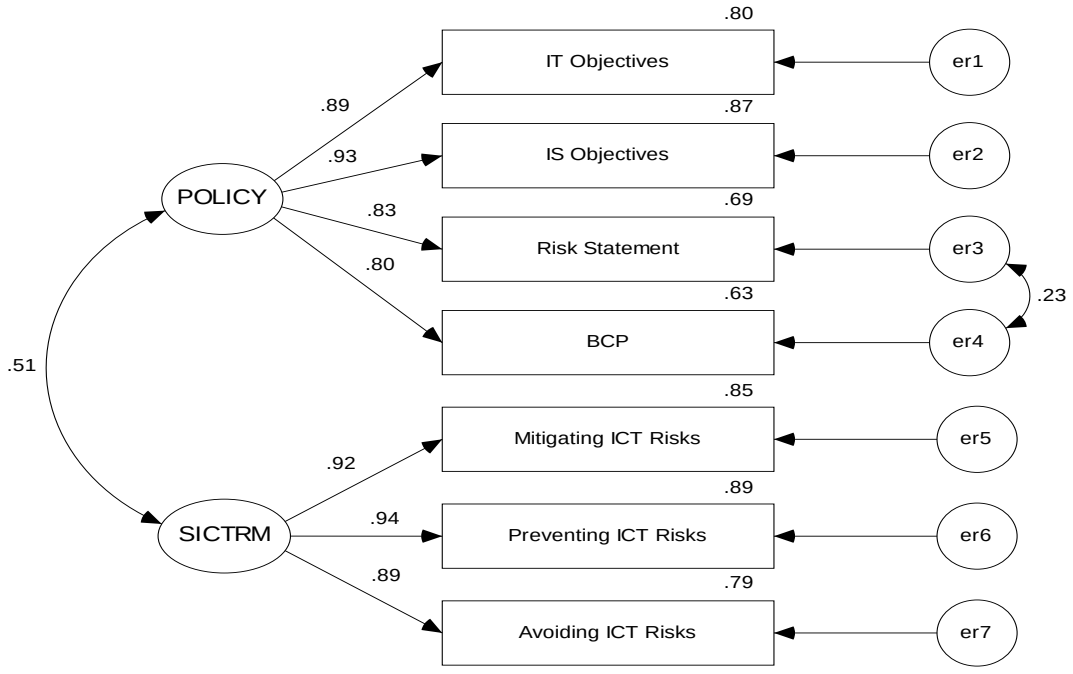


Figure 7-23: Discriminant validity of POLICY and SICTRM

According to the assessment of the dimensions, the POLICY dimension was tested with the SICTRM dimension to confirm that both dimensions are different from each other.

Table 7-37: POLICY and SICTRM for discriminant validity test

POLICY					SICTRM					
Indicator	λ	λ^2	ε	AVE	Indicator	λ	λ^2	ε	AVE	ρ^2
policy1	0.893	0.797	0.290		sictrm1	0.92	0.846	0.180		
policy2	0.932	0.868	0.188		sictrm2	0.942	0.888	0.105		
policy3	0.831	0.691	0.575		sictrm3	0.887	0.788	0.212		
policy4	0.797	0.635	0.570							
sum		2.991	1.623	0.648			2.522	0.497	0.835	0.260

The AVE values of POLICY and SICTRM are greater than the squared correlation between the dimensions, as shown in Table 7-37. Thus, both the POLICY and SICTRM dimensions held discriminant validity.

7.9.7 Human resource management and planning, and organisational information security (HRMP and OS)

As outlined in Figure 7-24, discriminant validity was used to test the correlation between HRMP and OS. The test found that the correlation (.87) between HRMP and OS was over .80.

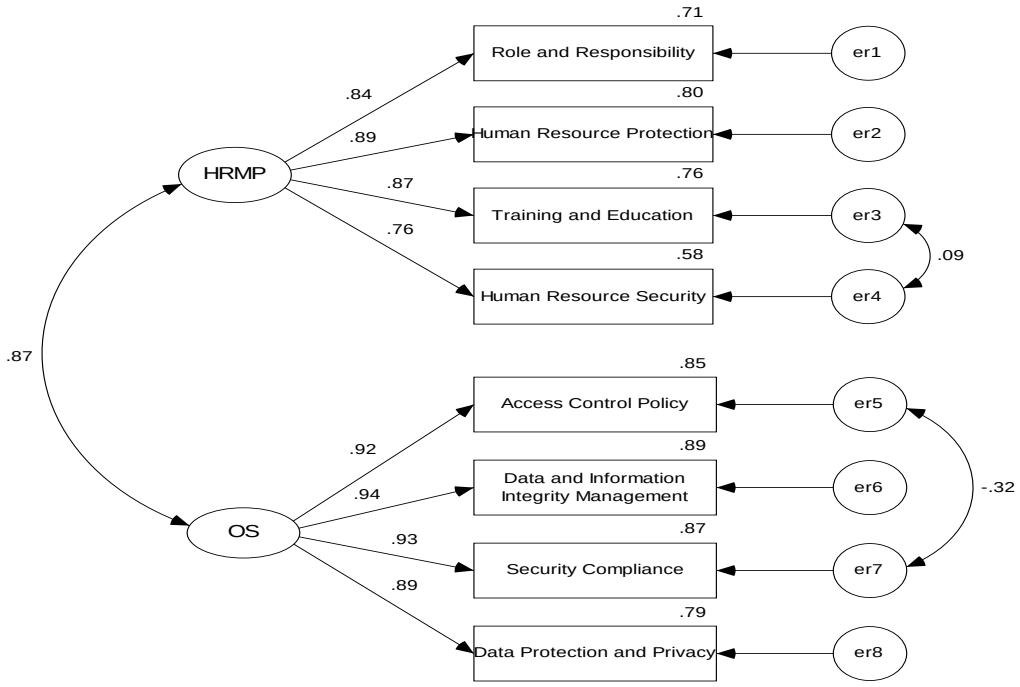


Figure 7-24: Discriminant validity of HRMP and OS

According to the assessment of the dimensions, the HRMP dimension was tested with the OS dimension to confirm that both dimensions are different from each other. The AVE value of HRMP did not meet the requirement to be lower than the squared correlation between the dimensions, as shown in Table 7-38.

Table 7-38: HRMP and OS for discriminant validity test

HRMP					OS					
Indicator	λ	λ^2	ε	AVE	Indicator	λ	λ^2	ε	AVE	ρ^2
hrmp1	0.844	0.712	0.510		os2	0.922	0.850	0.153		
hrmp2	0.893	0.797	0.299		os3	0.945	0.893	0.116		
hrmp3	0.872	0.761	0.385		os4	0.933	0.870	0.165		
hrmp4	0.759	0.576	0.490		os5	0.891	0.793	0.31		
sum		2.846	1.684	0.628			3.406	0.744	0.821	0.762

This indicated that both dimensions related to one and only one dimension as an example of unidimensionality (O'Leary-Kelly & Vokurta 1998). Thus, the researcher combined the two dimensions HRMP and OS to form a new factor called organisation information security management (OSM) (ISO/IEC 2005). Before combining them, they had to be retested using EFA, Cronbach's Alpha and CFA sequentially in order to confirm OSM as the new factor.

EFA was used to combine HRMP with OS to form OSM as a new factor. Table 7-39 depicts that entire indicators were extracted to only one factor, OSM, with high Cronbach's Alpha of .953 indicating good internal consistency. Moreover, the factor loadings were greater than .60 as exploratory research. However, this EFA was also used to confirm the new factor with CFA.

Table 7-39: EFA to combine HRMP and OS dimensions to form OSM

Total Variance Explained							Factor Matrix[a]	Communalities		Cronbach's Alpha (8 items)
Indicator	Initial Eigenvalues			Extraction Sums of Squared Loadings			Factor Loading (with and without rotation)	Initial	Extraction	
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %				
hrmp1	6.103	76.282	76.282	5.802	72.528	72.528	.787	.671	.619	.953
hrmp2	.587	7.336	83.617				.800	.739	.640	
hrmp3	.425	5.316	88.934				.794	.713	.630	
hrmp4	.256	3.203	92.137				.768	.610	.589	
os2	.206	2.575	94.712				.917	.811	.840	
os3	.174	2.174	96.886				.936	.862	.876	
os4	.152	1.903	98.789				.902	.825	.814	
os5	.097	1.211	100.000				.891	.775	.794	

Extraction Method: Maximum Likelihood

a. One factor extracted. Four iterations required.

As depicted in Figure 7-25, the OSM congeneric measurement model represented each reliable indicator. The indicators of OS were more reliable than the indicators of HRMP, as shown in Table 7-40.

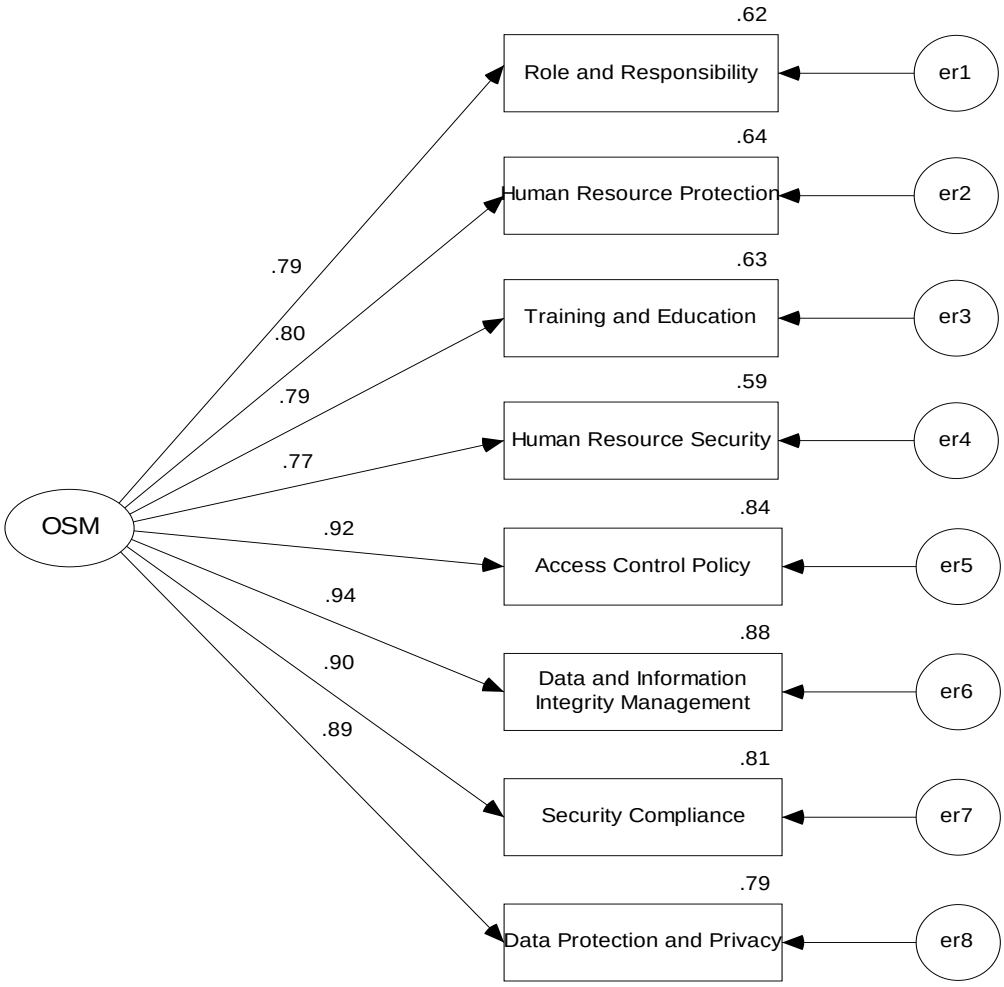


Figure 7-25: OSM congeneric measurement model

Table 7-40: Comparison of the squared multiple correlations for all indicators of OSM

Indicator			Former Factor Name		Standardised Regression Weights		Squared Multiple Correlations		OSM Cronbach's Alpha (4 items)
					OS	HRMP	OS	HRMP	
osm1	hrmp1	<-	OS	HRMP	.917	.787	.840	.619	9.53
osm2	hrmp2	<-	OS	HRMP	.936	.800	.876	.640	
osm3	hrmp3	<-	OS	HRMP	.902	.794	.814	.630	
osm4	hrmp4	<-	OS	HRMP	.891	.768	.794	.589	

Therefore, the researcher dropped the indicators of HRMP and retained only the indicators of OS, which represented the same meaning of the factor, as illustrated in Figure 7-26. As Figure 7-26 shows, the OSM congeneric measurement model modification indicates that the squared multiple correlations for the four indicators of OS

were greater than .79, which suggests that OSM accounts for over 79% of the variance in each of the indicators. This means that they are good measures of the dimension OSM.

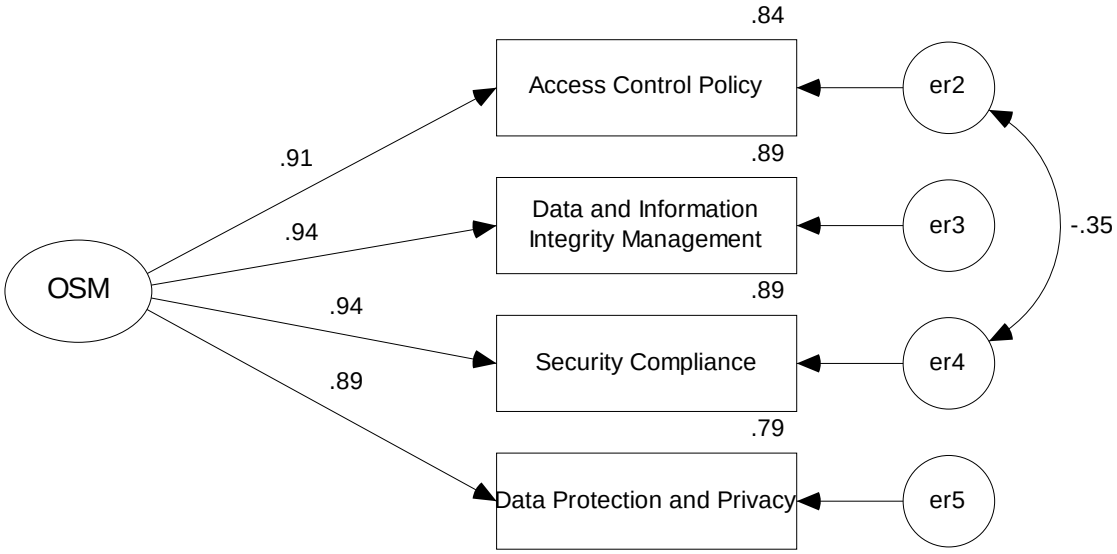


Figure 7-26: OSM congeneric measurement model modifications

With regard to the squared multiple correlations of OSM between OS and HRMP, all four indicators of OS represent better values than those of HRMP. The four OS indicators also demonstrate good reliability of OSM. Thus, OSM was a new factor generated from HRMP and OS to be a latent variable in this research. This can also be accepted to revalidate discriminant validity with other dimensions again in order to ensure that all dimensions hold discriminant validity. This is outlined in the following section.

7.9.8 The corporate level plan and the operational level plan (CLP and OLP)

According to Figure 7-27, discriminant validity was used to test the correlation between CLP and OLP. It was found that the correlation between CLP and OCLP was over .90.

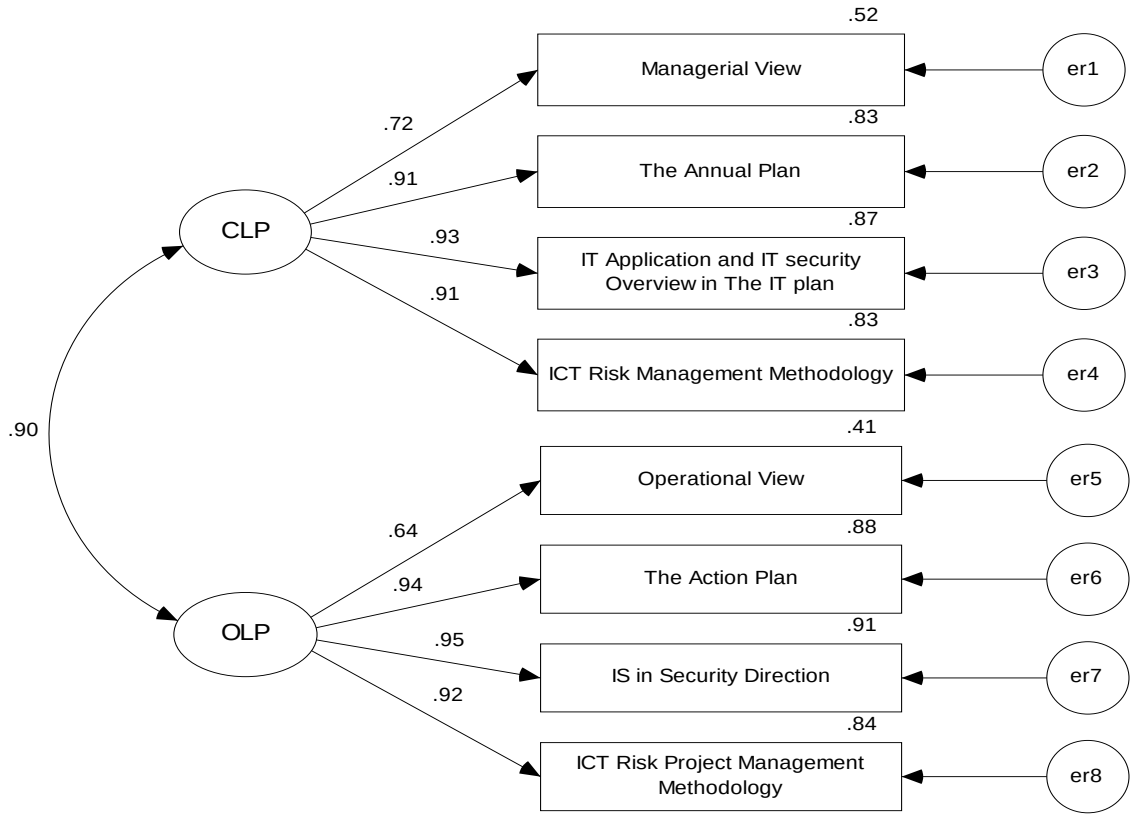


Figure 7-27: CLP and OLP for discriminant validity test

According to the assessment of the dimensions, the CLP dimension was tested with the OLP dimension to confirm that both dimensions are different from each other. The AVE values of CLP and OLP did not meet the requirements to be lower than the squared correlation between the dimensions, as shown in Table 7-41. Thus, both the CLP and OLP dimensions were merged to create a new factor, ELP, or the enterprise level plan.

Table 7-41: CLP and OLP for discriminant validity test

CLP					OLP					
Indicator	λ	λ^2	ε	AVE	Indicator	λ	λ^2	ε	AVE	ρ^2
clp1	0.719	0.520	0.825		olp1	0.642	0.412	1.107		
clp2	0.913	0.833	0.204		olp2	0.936	0.875	0.190		
clp3	0.931	0.866	0.189		olp3	0.953	0.909	0.162		
clp4	0.910	0.828	0.234		olp4	0.918	0.843	0.267		
sum		3.047	1.452	0.677			3.039	1.726	0.638	0.808

This indicated that the two dimensions related to one and only one dimension as a form of unidimensionality (O'Leary-Kelly & Vokurta 1998). Before combining the dimensions, they needed to be retested using EFA, Cronbach's Alpha and CFA sequentially in order to confirm ELP as the new factor. Organisation theory was used to name the enterprise level plan (ELP), based on the claim of Christensen et al. (2007, p. 27) that 'reforming public organizations through restructuring does not necessarily lead to either centralization (or the corporate level plan) or decentralization (or the operational plan), but may involve both simultaneously'.

Table 7-42 reveals that entire indicators were extracted to only one factor, namely ELP, with a high Cronbach's Alpha of .951 indicating good internal consistency. The factor loadings are greater than .60 as exploratory research. However, this EFA was also used to confirm the new factor with CFA.

Table 7-42: EFA to combine CLP and OLP dimensions to form ELP

Total Variance Explained							Factor Matrix[a]	Communalities		Cronbach's Alpha (8 items)
Indicator	Initial Eigenvalues			Extraction Sums of Squared Loadings			Factor Loading (with and without rotation)	Initial	Extraction	
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %				
clp1	6.054	75.676	75.676	5.777	72.213	72.213	.724	.611	.525	.951
clp2	.673	8.412	84.088				.879	.792	.772	
clp3	.429	5.362	89.450				.888	.813	.789	
clp4	.302	3.773	93.223				.864	.790	.746	
olp1	.177	2.215	95.439				.658	.537	.433	
olp2	.141	1.768	97.206				.919	.835	.845	
olp3	.127	1.583	98.789				.925	.861	.855	
olp4	.097	1.211	100.000				.900	.812	.811	

Extraction Method: Maximum Likelihood.

a. One factor extracted. Four iterations required.

As depicted in Figure 7-28, the ELP congeneric measurement model represented each reliable indicator.

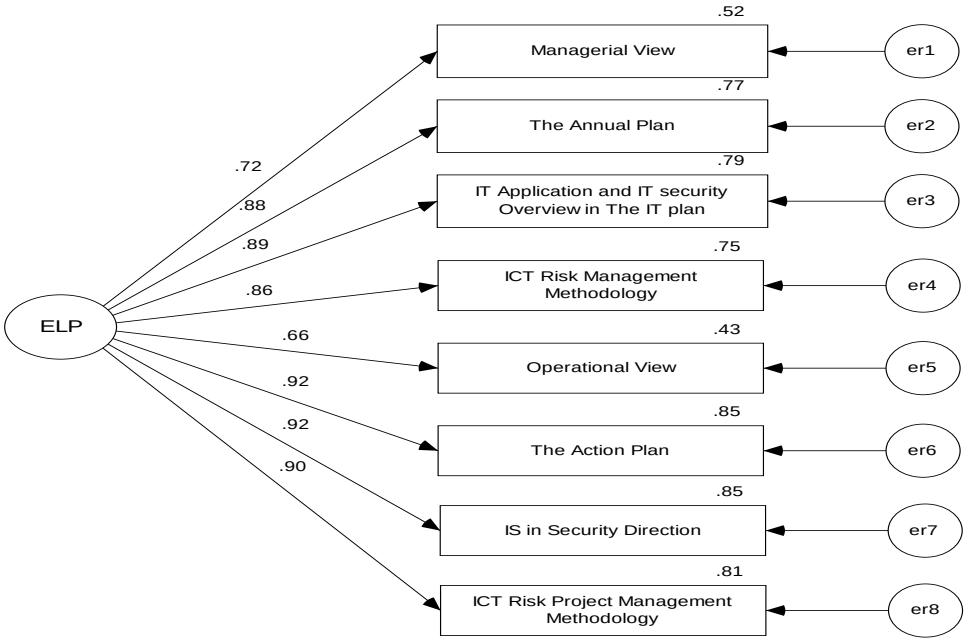


Figure 7-28: ELP congeneric measurement model

The researcher dropped four indicators (clp1=Managerial View, clp2=The corporate plan, clp4=ICT Risk Management Methodology and olp1=Operational View) for which the factor loadings were less than .70 and due to problematic issues in the modification indices (MI), and retained only those indicators that explained ELP by over 70%, as shown in Figure 7-29.

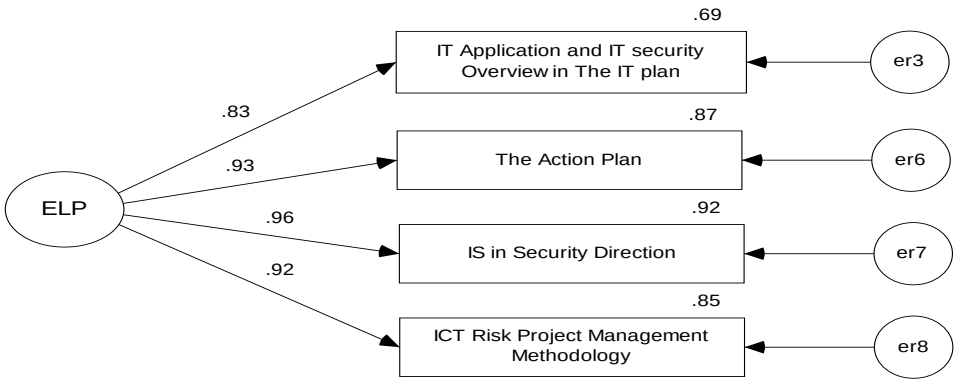


Figure 7-29: ELP congeneric measurement model modifications

With regard to the squared multiple correlations of ELP between CLP and OLP, all four indicators represent good reliability of ELP, as shown in Table 7-43. Thus, ELP was the new factor generated from CLP and OLP to be a latent variable in this research.

Table 7-43: ELP congeneric measurement model with indices

Indicator		Factor	λ	R^2	Model Fit		Cronbach's Alpha (4 items)
					Indices	After Rectifying	
elp1	<---	ELP	.830	.689	χ^2/df (2.934/2)	1.467	.950
elp2	<---	ELP	.932	.869	P-value	.661	
elp3	<---	ELP	.957	.915	TLI	.998	
elp4	<---	ELP	.920	.846	CFI	.999	
					RMSEA	.039	
					SRMR	.005	
					HOELTER		
					0.05	615	
					Multivariate		
					Kurtosis	28.919	
					Critical Ratio	36.269	

The ELP congeneric measurement model modifications indicated that the squared multiple correlations are greater than .69, which suggests that ELP accounts for over 69% of the variance in each of the indicators. This means that they are good measure of the dimension ELP.

7.9.9 Organisational information security management and the enterprise level plan (OSM and ELP)

As shown in Figure 7-30, discriminant validity was used to test the correlation between OSM and ELP. It was found that the correlation between OSM and ELP was .88.

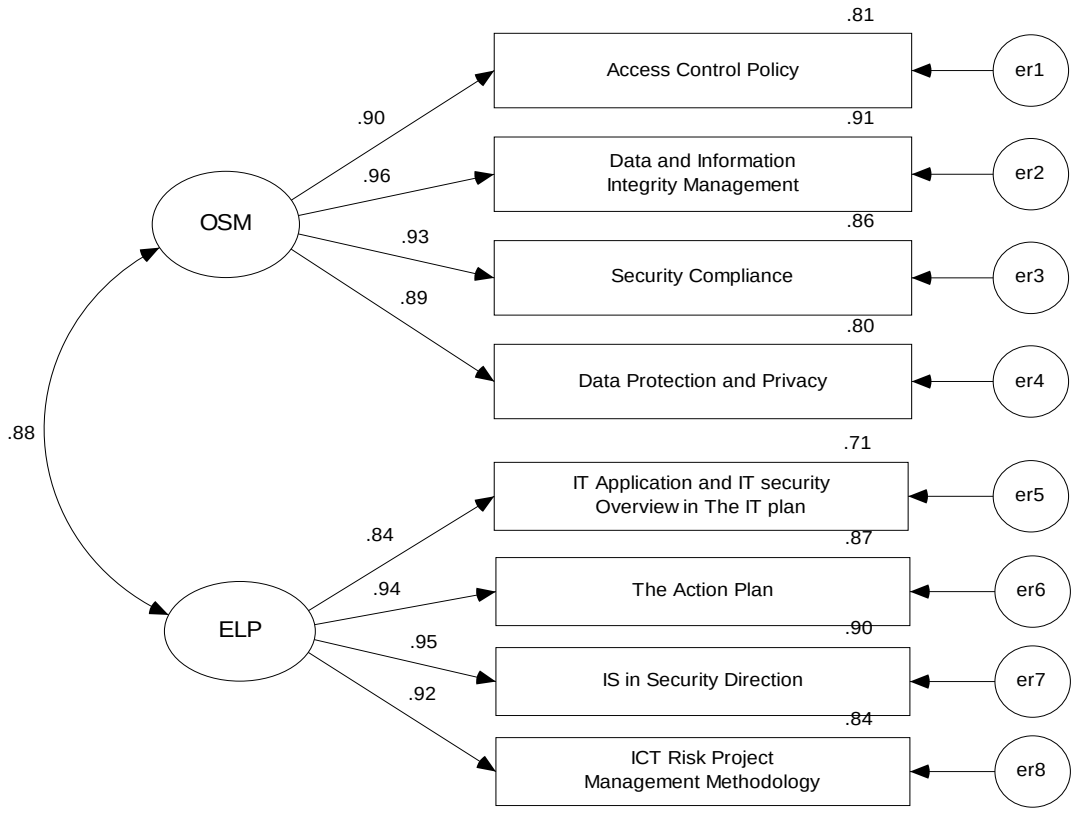


Figure 7-30: OSM and ELP for discriminant validity test

According to the assessment of the dimensions above, the OSM dimension was tested with the ELP dimension to confirm that both dimensions are different from each other. The AVE value of ELP did not meet the requirement to be lower than the squared correlation between the dimensions, as shown in Table 7-44. Thus, OSM was used to form a new factor, ESP, because of its high AVE value.

Table 7-44: OSM and ELP for discriminant validity test

OSM					ELP					
Indicator	λ	λ^2	ε	AVE	Indicator	λ	λ^2	ε	AVE	ρ^2
osm1	0.897	0.81	0.198		elp1	0.844	0.713	0.407		
osm2	0.955	0.91	0.094		elp2	0.935	0.875	0.190		
osm3	0.927	0.86	0.178		elp3	0.949	0.901	0.175		
osm4	0.892	0.8	0.307		elp4	0.918	0.843	0.267		
sum		3.373	0.777	0.813			3.332	1.039	0.762	0.781

This suggested that both dimensions related to one and only one dimension as an example of unidimensionality (O'Leary-Kelly & Vokurta 1998). Thus, the researcher combined the two dimensions OSM and ELP to form the enterprise information security plan (ESP) as a new factor. The combination of organisational security management and the enterprise level plan implies that the samples manage ICT risks by using information security at both the corporate level (i.e. a top-down approach) and the operational level

(i.e. a bottom-up approach) (Solms 2005a). Consequently, the new name ESP represents the data more clearly. Before combining the dimensions, it was necessary that they be retested using EFA, Cronbach's Alpha and CFA sequentially in order to confirm ESP as the new factor.

Table 7-45 indicates that only one factor was extracted to only one factor, ELP, with a high Cronbach's Alpha of .966, demonstrating good internal consistency. The factor loadings were greater than .60 as exploratory research. However, this EFA was also used to confirm the new factor using CFA.

Table 7-45: EFA to combine OSM and ELP dimensions to form ESP

Total Variance Explained							Factor Matrix[a]	Communalities		Cronbach's Alpha (8 items)
Indicator	Initial Eigenvalues			Extraction Sums of Squared Loadings			Factor Loading (with and without rotation)	Initial	Extraction	
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %				
osm1	6.512	81.396	81.396	6.300	78.749	78.749	.876	.777	.767	.966
osm2	.519	6.490	87.886				.927	.870	.859	
osm3	.275	3.443	91.329				.902	.842	.813	
osm4	.202	2.519	93.848				.878	.784	.771	
elp1	.176	2.196	96.044				.855	.726	.731	
elp2	.128	1.602	97.646				.893	.840	.798	
elp3	.106	1.330	98.976				.895	.861	.801	
elp4	.082	1.024	100.000				.872	.821	.761	

Extraction Method: Maximum Likelihood.

a. One factor extracted. Four iterations required.

As shown in Figure 7-31, the ESP congeneric measurement model represents each reliable indicator. Over 73% of the variance in each of the indicators is explained by the ESP congeneric measurement model. However, the MIs revealed that the model did not fit.

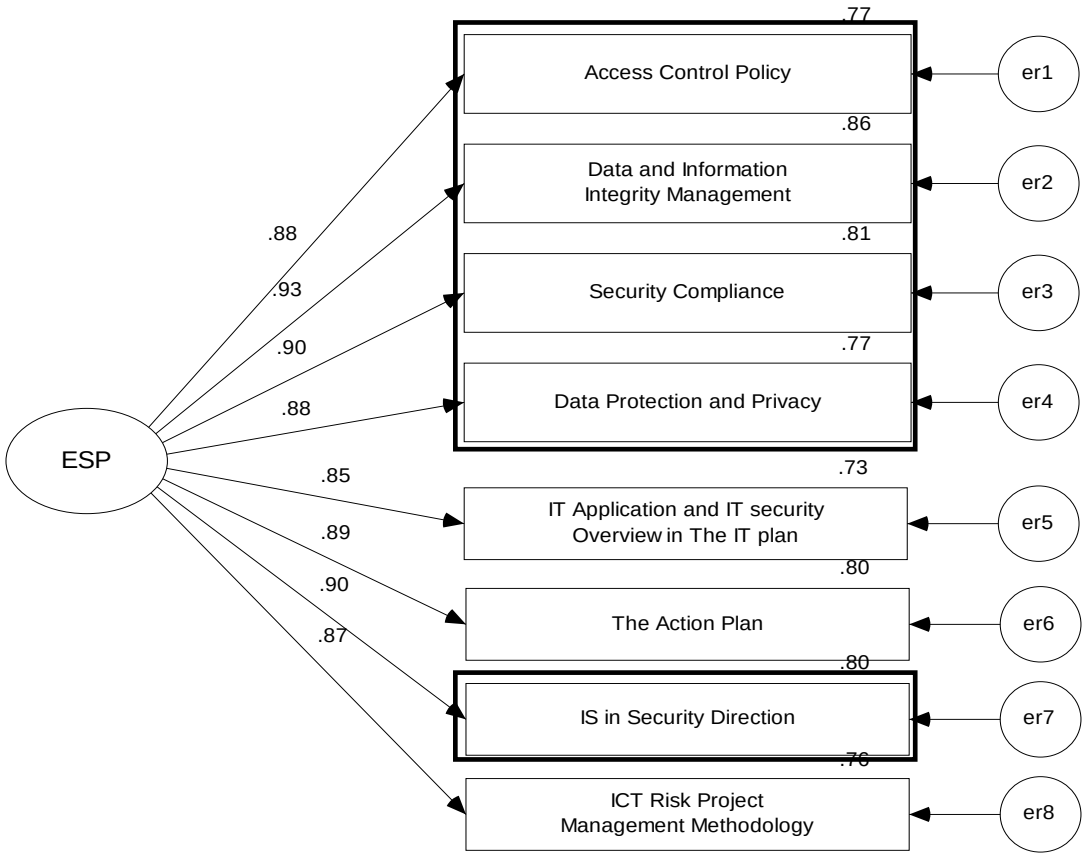


Figure 7-31: ESP congeneric measurement model

Thus, this congeneric measurement model had to be rectified in order to confirm the indicators for this ESP as a new factor, as depicted in Figure 7-32. The researcher dropped three indicators (elp1=IT Applications and IT Security Overview in the IT plan, elp2=The Action Plan, and elp4=ICT Project Risk Management Methodology) based on a problematic issue with the modification indices. As a result, the ESP congeneric measurement model depicted the squared multiple correlations to be over .68, which suggests that ELP accounts for over 68% of the variance in each of the indicators. This means they are a good measure of the dimension ESP.

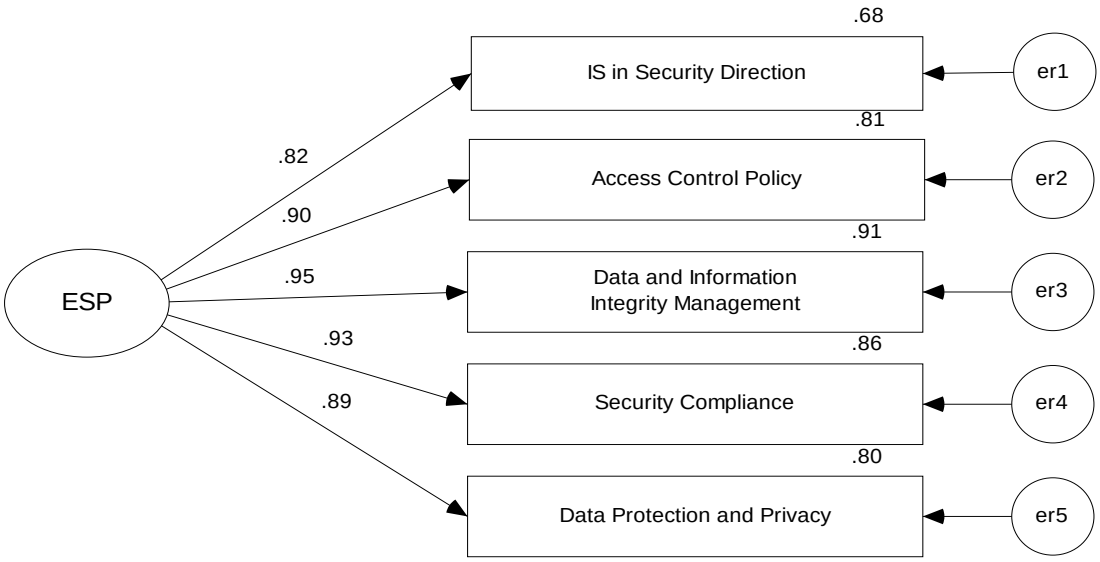


Figure 7-32: ESP congeneric measurement model modifications

With regard to the squared multiple correlations of ESP between OSM and ELP, five indicators represented good reliability of ESP, as shown in Table 7-46. Thus, ESP was the new factor generated from OSM and ELP to be a latent variable in this research.

Table 7-46: ESP congeneric measurement model with indices

Indicator		Factor	λ	R^2	Model Fit		Cronbach's Alpha (5 items)
					Indices	After Rectifying	
esp1	<---	ESP	.823	.678	χ^2/df(10.966/5)	2.193	.950
esp2	<---	ESP	.898	.806	P-value	.423	
esp3	<---	ESP	.954	.910	Multivariate		
esp4	<---	ESP	.928	.862	Kurtosis	31.006	
esp5	<---	ESP	.892	.795	Critical Ratio	32.201	
					TLI	.993	
					CFI	.996	
					RMSEA	.063	
					SRMR	.007	
					HOELTER		
					0.05	304	

Through the combination of HRMP, OS, CLP and OLP, ESP was generated as a new factor to be tested for discriminant validity with the other dimensions in order to ensure that all dimensions hold discriminant validity. This process is outlined in the following sections.

7.9.10 The enterprise information security plan and organisational policy (ESP to POLICY)

As revealed in Figure 7-33, discriminant validity was used to test the correlation between ESP and POLICY. It was found that the correlation (.78) between ESP and POLICY was less than .80.

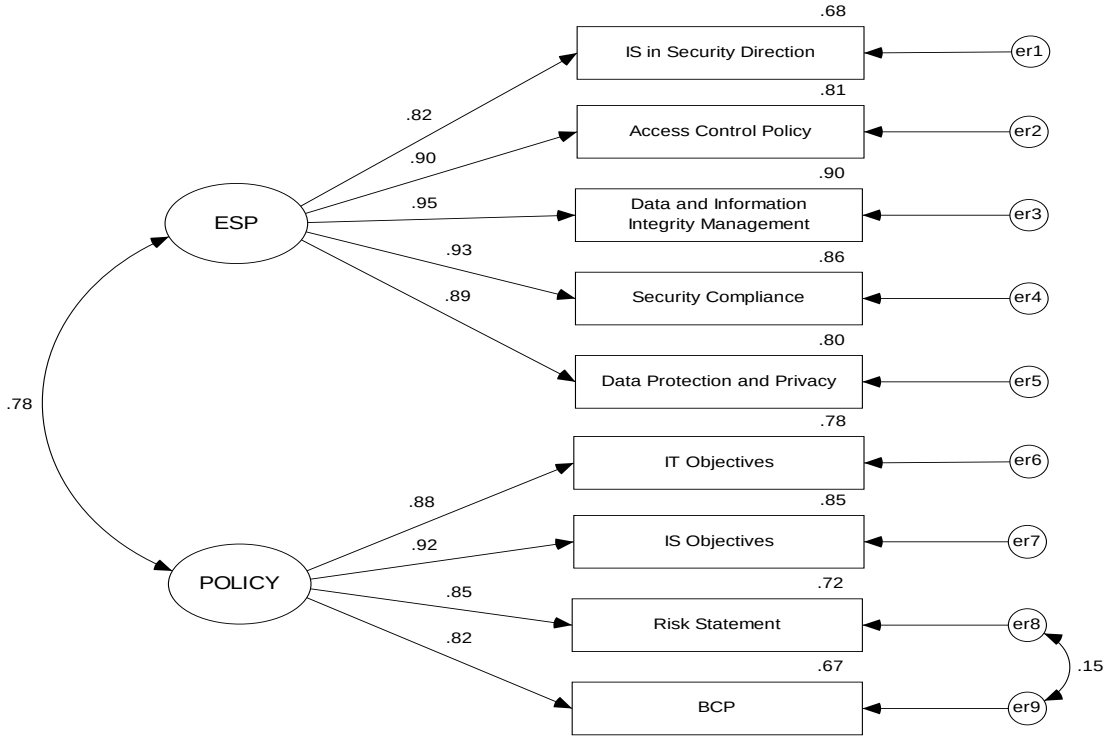


Figure 7-33: Discriminant validity between ESP and POLICY

According to the assessment of the dimensions, the ESP dimension was tested with the POLICY dimension to confirm that both dimensions are different from each other.

Table 7-47: ESP and POLICY for discriminant validity test

ESP					POLICY					
Indicator	λ	λ^2	ε	AVE	Indicator	λ	λ^2	ε	AVE	ρ^2
esp1	0.823	0.678	0.573		policy1	0.882	0.778	0.316		
esp2	0.901	0.811	0.192		policy2	0.922	0.850	0.214		
esp3	0.951	0.904	0.103		policy3	0.849	0.721	0.519		
esp4	0.930	0.864	0.172		policy4	0.816	0.666	0.521		
esp5	0.892	0.797	0.305							
sum		4.054	1.345	0.751			3.015	1.570	0.658	0.612

The AVE values of POLICY and ESP are greater than the squared correlation between the dimensions, as shown in Table 7-47. Thus, both the ESP and POLICY dimensions held discriminant validity.

7.9.11 The enterprise information security plan and management of ICT resources (ESP and IT)

As shown in Figure 7-34, discriminant validity was used to test the correlation between ESP and IT. The test found that the correlation (.80) between ESP and IT was equal to .80.

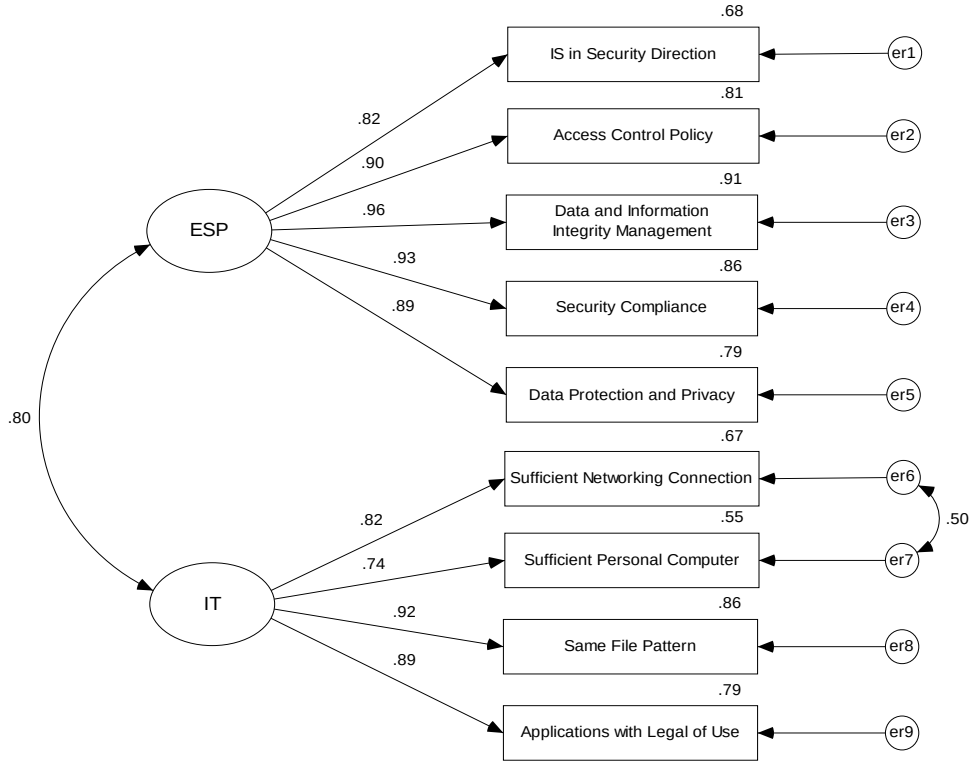


Figure 7-34: Discriminant validity between ESP and IT

According to the assessment of the dimensions above, the ESP dimension was tested with the IT dimension to confirm that both dimensions are different from each other.

Table 7-48: ESP and IT for discriminant validity test

ESP					IT					
Indicator	λ	λ^2	ε	AVE	Indicator	λ	λ^2	ε	AVE	ρ^2
esp1	0.823	0.677	0.574		it1	0.816	0.666	0.459		
esp2	0.897	0.805	0.198		it2	0.741	0.550	0.690		
esp3	0.955	0.912	0.095		it3	0.925	0.855	0.168		
esp4	0.929	0.863	0.174		it4	0.888	0.788	0.246		
esp5	0.890	0.792	0.312							
sum		4.049	1.353	0.750			2.859	1.563	0.647	0.632

The AVE values of ESP and IT are greater than the squared correlation between the dimensions, as shown in Table 7-48. Thus, both the ESP and IT dimensions held discriminant validity.

7.9.12 The enterprise information security plan and successful ICT risk management (ESP and SICTRM)

As outlined in Figure 7-35, discriminant validity was used to test the correlation between ESP and SICTRM. It was found that the correlation (.66) between ESP and SICTRM was less than .80.

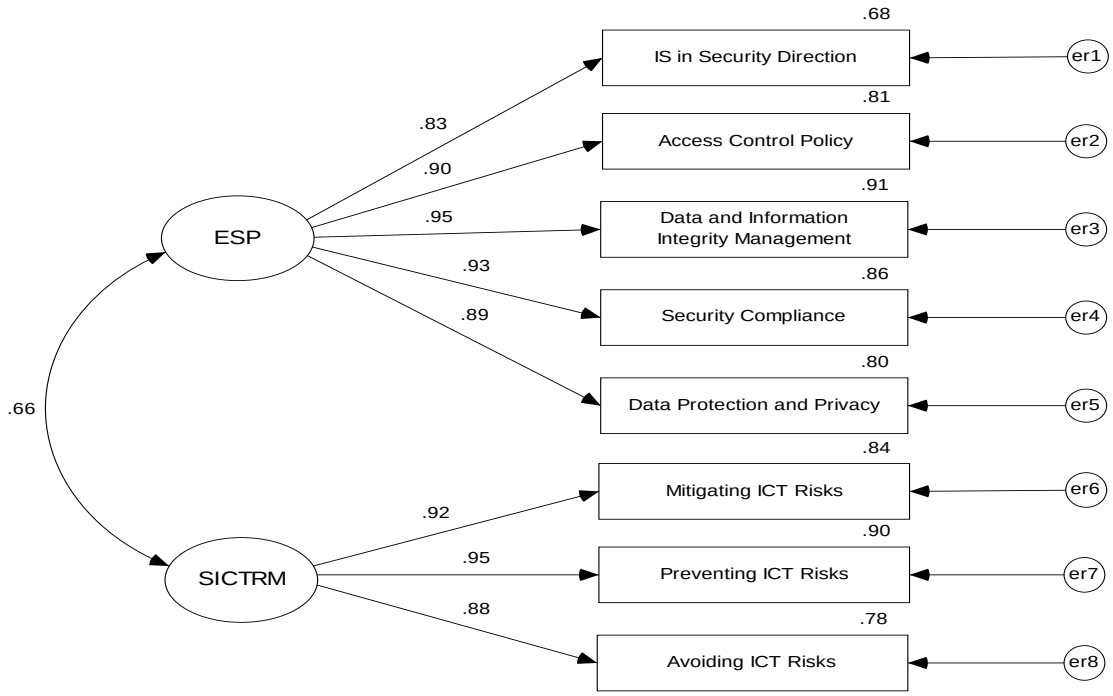


Figure 7-35: Discriminant validity between ESP and SICTRM

According to the assessment of the dimensions above, the ESP dimension was tested with the SICTRM dimension to confirm that both dimensions are different from each other.

Table 7-49: ESP and SICTRM for discriminant validity test

ESP					SICTRM					
Indicator	λ	λ^2	ε	AVE	Indicator	λ	λ^2	ε	AVE	ρ^2
esp1	0.825	0.681	0.566		sictrm1	0.917	0.841	0.186		
esp2	0.899	0.809	0.194		sictrm2	0.947	0.896	0.098		
esp3	0.952	0.906	0.102		sictrm3	0.885	0.783	0.216		
esp4	0.929	0.863	0.174							
esp5	0.892	0.796	0.306							
sum		4.055	1.342	0.751			2.520	0.500	0.834	0.432

The AVE values of ESP and SICTRM are greater than the squared correlation between the dimensions, as shown in Table 7-49. Thus, both the ESP and SICTRM dimensions held discriminant validity.

7.9.13 Management of ICT resources and successful ICT risk management (IT and SICTRM)

As depicted in Figure 7-36, discriminant validity was used to test the correlation between IT and SICTRM. It was found that the correlation (.65) between IT and SICTRM was less than .80.

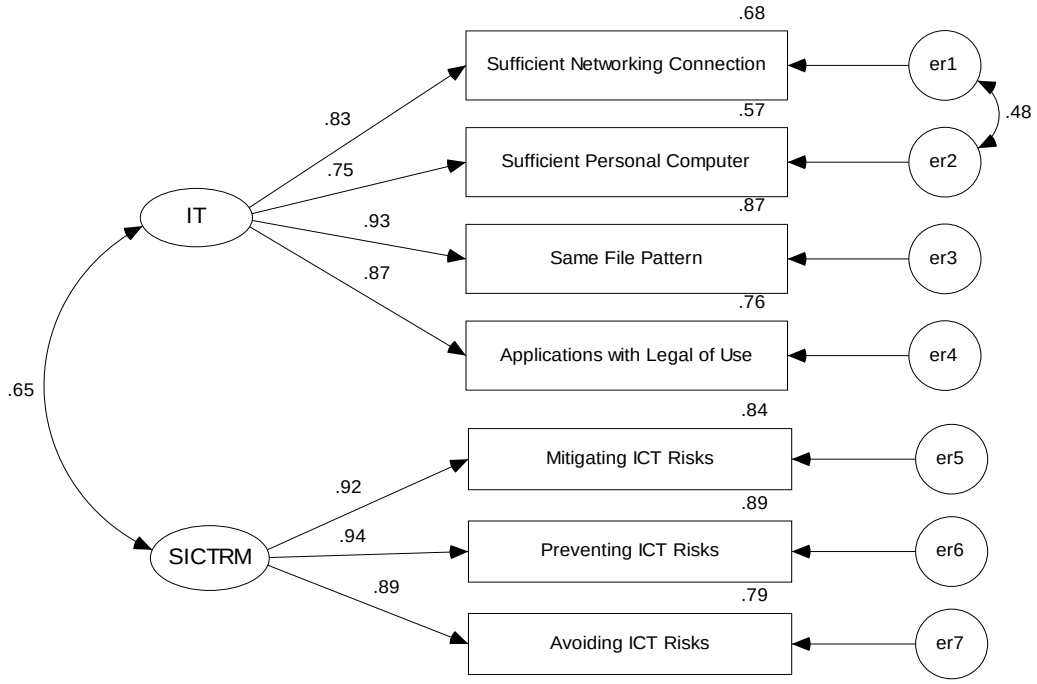


Figure 7-36: Discriminant validity between IT and SICTRM

According to the assessment of the dimensions above, the IT dimension was tested with the SICTRM dimension to confirm that both dimensions are different from each other. The AVE values of IT and SICTRM are greater than the squared correlation between the dimensions, as shown in Table 7-50. Thus, both the IT and SICTRM dimensions held discriminant validity.

Table 7-50: IT and SICTRM for discriminant validity test

IT					SICTRM					
Indicator	λ	λ^2	ε	AVE	Indicator	λ	λ^2	ε	AVE	ρ^2
it1	0.826	0.683	0.436		sictrm1	0.919	0.845	0.182		
it2	0.755	0.570	0.659		sictrm2	0.941	0.885	0.108		
it3	0.931	0.866	0.156		sictrm3	0.890	0.793	0.207		
it4	0.872	0.760	0.279							
sum		2.879	1.530	0.653			2.523	0.497	0.835	0.420

As seen in Table 7-51, the AVE summary lists the discriminant validity among the factors (latent variables) in this model.

Table 7-51: AVE measures summary

Factor			AVE			ρ2
POLICY	<--->	IT	0.650	<--->	0.647	0.370
POLICY	<--->	ESP	0.658	<--->	0.751	0.612
POLICY	<--->	SICTRM	0.648	<--->	0.835	0.260
IT	<--->	ESP	0.647	<--->	0.750	0.632
IT	<--->	SICTRM	0.653	<--->	0.835	0.420
ESP	<--->	SICTRM	0.751	<--->	0.834	0.432

After evaluating discriminant validity, it was found that all AVE measures were higher than ρ^2 for all factors. Thus, all dimensions were found to hold discriminant validity and were ready to be evaluated in the measurement model.

7.10 Stage VII: The measurement model (dimension validity)

Figure 7-37 represents the new modified measurement model that was used to determine the reliability of the instrument along with its indicators.

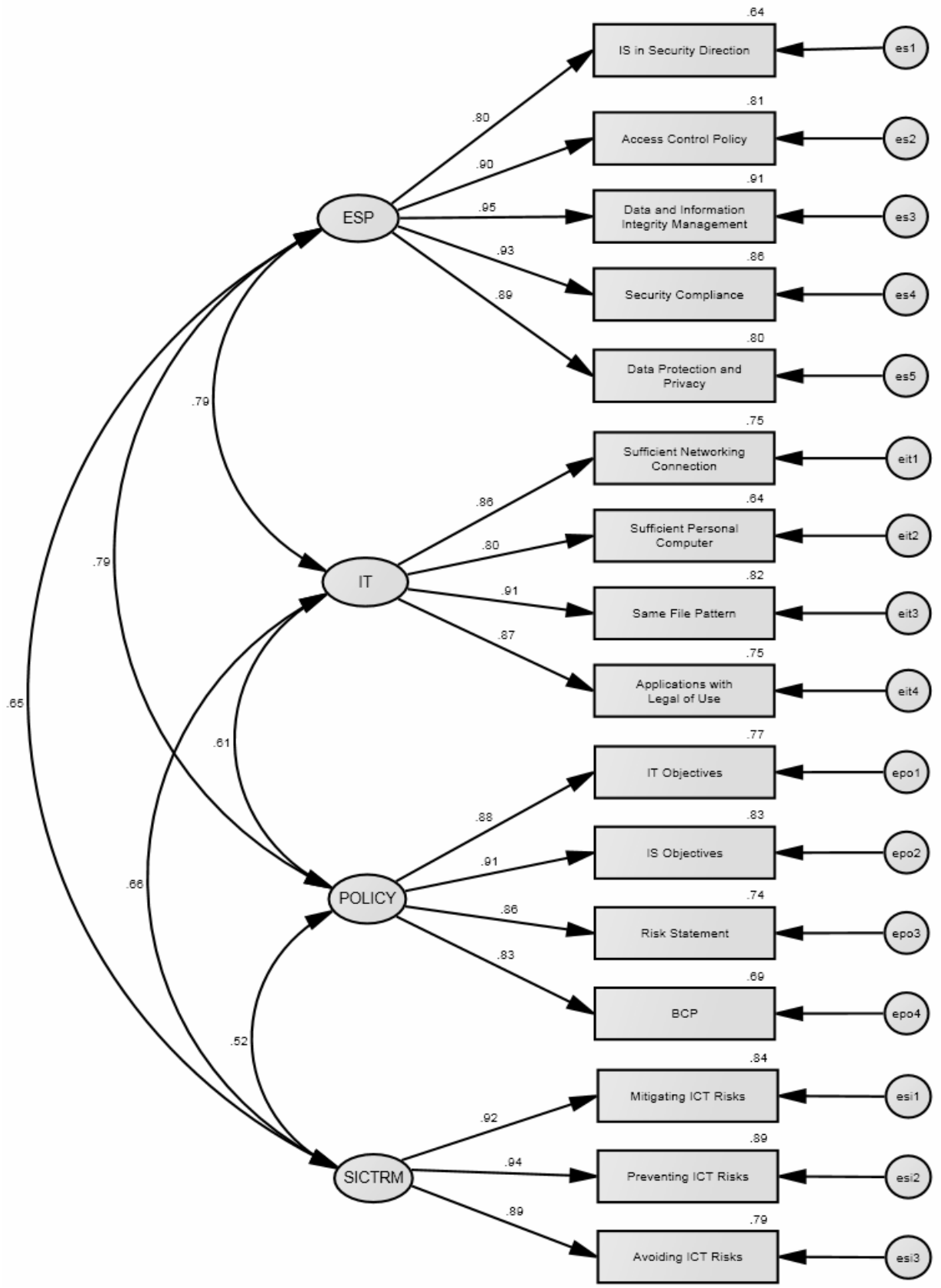


Figure 7-37: The measurement model of successful ICT risk management

The results indicate that the model was not a good fit, with the values of χ^2/df(304.948/98)=3.112, p=.004, TLI=.950, CFI=.959, RMSEA=.084, SRMR=.040, and HOELTER=121 with a confidence level of 95% (see Table 7-52).

Table 7-52: The measurement model indices before rectifying

Indicator		Factor	λ	R^2	Model Fit		Cut-off value Requirement
					Indices	Before	
esp1	<---	ESP	.801	.642	χ^2/df (304.948/98)	3.112	<3
esp2	<---	ESP	.902	.813	P-value	.004	>.05
esp3	<---	ESP	.952	.907	TLI	.950	≥.95
esp4	<---	ESP	.927	.858	CFI	.959	≥.95
esp5	<---	ESP	.892	.796	RMSEA	.084	<.06
it1	<---	IT	.865	.748	SRMR	.040	<.08
it2	<---	IT	.798	.637	HOELTER		
it3	<---	IT	.907	.822	P=0.05	121	≥200
it4	<---	IT	.866	.751	Multivariate normal distribution test		
policy1	<---	POLICY	.876	.768	Kurtosis	214.038	
policy2	<---	POLICY	.913	.834	Critical ratio of kurtosis	77.491	>1.96
policy3	<---	POLICY	.861	.741			
policy4	<---	POLICY	.831	.691			
sictrm1	<---	SICTRM	.919	.844			
sictrm2	<---	SICTRM	.887	.891			
sictrm3	<---	SICTRM	.892	.786			

Hair et al. (2006) suggest that the reliability of an instrument is indicated by the factor loading of all indicators, the standardised residual, the critical ratio (CR) and the modification indices. Three measures were applied in this research to modify the measurement model to ensure it is a good fit. The measurement model modification firstly determined that the factor loadings should be greater than .7; the factor loadings of all indicators were indeed greater than .7. Next the standardised residuals and critical ratio (CR) were the focus of the analysis.

Table 7-53 shows that all standardised residuals were less than 2.58. This indicates that the mean of standard errors in the sample data shows no discrepancy from the mean of standard errors in the population. Therefore, the measurement model replicates the sample data of this research; as a result, statistical values are estimated accurately.

Moreover, as presented in Table 7-54, the critical ratio (CR) or path coefficient (e.g. ESP --> esp1) in each path is greater than 1.96 for a regression weight, and that path is significant at 95% confidence interval (that is, its estimated path parameter is significant) (Garson 2009). Therefore, all paths in the measurement model are statistically significant.

Table 7-53: Standardised residual covariances

	esp5	sictrm3	sictrm2	sictrm1	policy4	policy3	policy2	policy1	it4	it3	it2	it1	esp4	esp3	esp2	esp1
esp5	.000															
sictrm3	-.806	.000														
sictrm2	.156	.042	.000													
sictrm1	.140	.019	-.038	.000												
policy4	.803	.628	1.139	1.498	.000											
policy3	-.098	-1.183	-.244	-.130	.336	.000										
policy2	-.133	-.920	-.211	.274	-.355	-.096	.000									
policy1	-.513	-.805	-.276	.573	-.249	-.270	.470	.000								
it4	.276	-.444	-.855	-.360	1.807	.338	.401	-.162	.000							
it3	-.135	-.263	-.278	.018	.914	.037	.042	-.278	.483	.000						
it2	-1.035	.049	.189	-.344	-.305	-1.241	-1.800	-1.609	-.491	-.366	.000					
it1	-.507	.616	.785	1.256	1.563	-.176	-.198	.139	-.604	-.297	1.562	.000				
esp4	.166	-.488	.299	.292	.709	.539	-.005	-.349	.465	.315	-1.089	.031	.000			
esp3	-.158	-.756	-.115	-.144	.871	.287	-.621	-.864	.784	.162	-1.174	-.214	.102	.000		
esp2	.074	-.417	.555	.694	1.428	.538	.053	-.024	.513	-.165	-.433	.135	-.270	.054	.000	
esp1	.356	-.832	.440	.416	.680	.878	-.360	-1.142	.955	.746	-1.052	-.879	-.445	.142	-.045	.000

Table 7-54: Critical ratio (t-value)

			Estimate	S.E.	C.R.	P				Estimate	S.E.	C.R.	P
esp1	<---	ESP	1.044	.062	16.708	***	it4	<---	IT	.934	.050	18.623	***
esp2	<---	ESP	.909	.045	20.171	***	policy1	<---	POLICY	1.047	.055	18.995	***
esp3	<---	ESP	.988	.044	22.214	***	policy2	<---	POLICY	1.091	.054	20.369	***
esp4	<---	ESP	1.043	.049	21.141	***	policy3	<---	POLICY	1.175	.064	18.466	***
esp5	<---	ESP	1.093	.055	19.806	***	policy4	<---	POLICY	1.039	.059	17.466	***
it1	<---	IT	1.013	.055	18.562	***	sictrm1	<---	SICTRM	.993	.048	20.629	***
it2	<---	IT	.988	.060	16.390	***	sictrm2	<---	SICTRM	.916	.042	21.611	***
it3	<---	IT	.977	.049	20.080	***	sictrm3	<---	SICTRM	.885	.046	19.448	***

Only modification indices were statistically performed to drop those indicators showing poor performance. It was determined that esp1 (IS in security direction), it2 (sufficient personal computer) and policy4 (BCP) should be discarded, thereby eradicating the problematic issue in MI. The final measurement model resulting from these changes is shown in Figure 7-38.

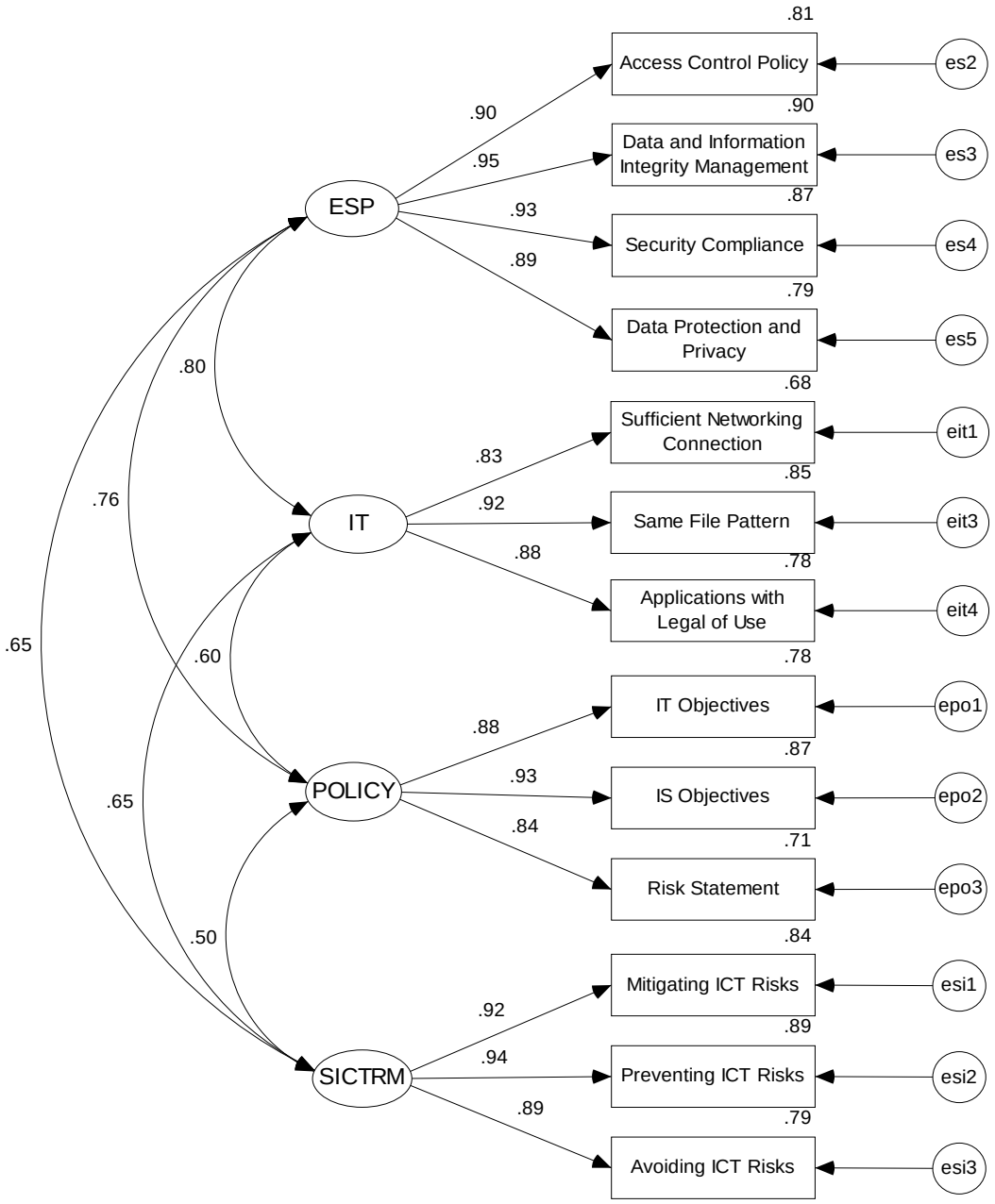


Figure 7-38: The measurement model modifications

The rectified measurement model revealed that all indicators displayed good reliability and all indicators represented their own dimension well. The squared multiple correlations for all indicator variables were greater than .68 (see Table 7-55). This suggested that the latent dimensions account for more than 68% of the variance in each of the indicators—thus, they are good measures of the dimensions. In other words, four

dimensions out of the seven which were originally based on the qualitative analysis were confirmed as factors for successful ICT risk management.

Table 7-55: The measurement model indices after rectifying

Indicator		Factor	λ	R^2	Coefficient		Model Fit		Cut-off value Requirement
					Alpha	H	Indices	After	
esp2	<---	ESP	.900	.810	0.953	0.959	χ^2/df (113.762/59)	1.928	<3
esp3	<---	ESP	.950	.903			P-value	.218	>.05
esp4	<---	ESP	.932	.869			TLI	.982	≥.95
esp5	<---	ESP	.890	.792			CFI	.987	≥.95
it1	<---	IT	.826	.682	0.905	0.918	RMSEA	.056	<.06
it3	<---	IT	.922	.849			SRMR	.029	<.08
it4	<---	IT	.881	.777			HOELTER		
policy1	<---	POLICY	.885	.783	0.912	0.927	P=0.05	207	≥200
policy2	<---	POLICY	.933	.871			Multivariate normal distribution test		
policy3	<---	POLICY	.843	.711			Kurtosis	151.610	
sictrm1	<---	SICTRM	.919	.845	0.939	0.944	Critical ratio of kurtosis	66.707	>1.96
sictrm2	<---	SICTRM	.943	.890					
sictrm3	<---	SICTRM	.887	.787					
All indicators					0.950	0.984			

However, each dimension was tested again using SEM in order to ensure that the four dimensions have a relationship with, and are significant for establishing, successful ICT risk management.

7.11 Stage VIII: Structural equation modelling (SEM)

The structural model was used to show that all factors represented their relevant dimensions. An analysis of SEM was performed with the maximum likelihood estimation method (MLE) in combination with the bootstrapping method (refer to pp. 181-182) to measure the relationship among the dimensions, in order to confirm or reject the research hypothesis, as presented in Figure 7-39.

The structural model indicates that (1) organisational policy has high impact on the management of ICT resources [.60] and (2) the enterprise information security plan [.44] when establishing (3) successful ICT risk management through the enterprise information security plan [.37] and through the management of ICT resources [.35]. In this regard, the impact of organisational policy on both the management of ICT resources and the enterprise information security plan is supported by strategic management theory (Wheelen & Hunger 2004). Organisational policy is defined as 'strategic formulation' at the level of the Board of Directors (Wheelen & Hunger 2004, P. 25). On

this account, organisational policy is driven by senior management as 'strategy implementation' to set the planning and management guidelines of organisations (Wheelen & Hunger 2004, p. 25). Therefore, this model reflects significant similarity to the theoretical concepts of organisational strategic management.

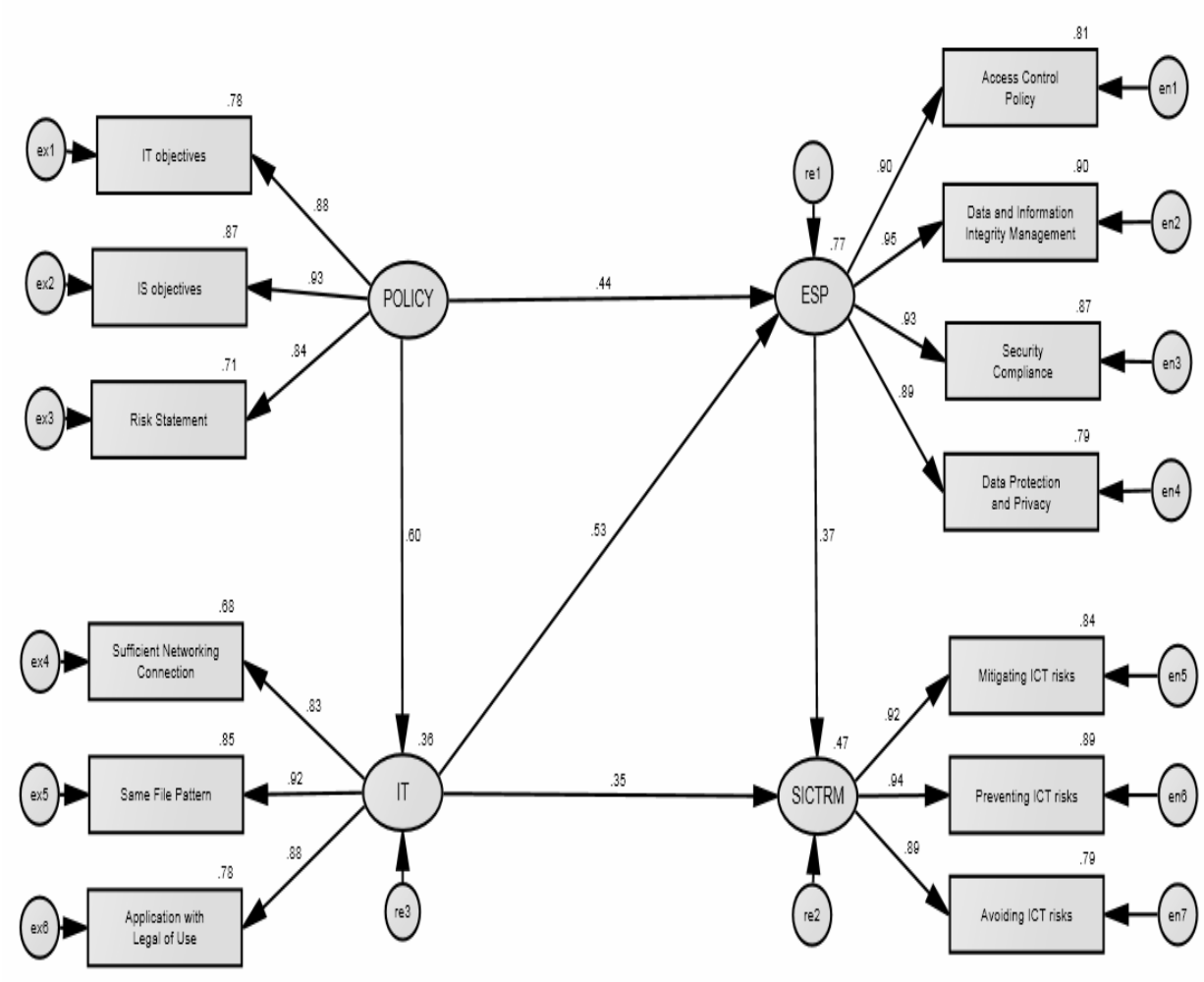


Figure 7-39: The structural model of successful ICT risk management

The outputs of the SEM indicated an overall good fit, with the values of χ^2/df(113.762/60)= 1.896, p=.251, TLI=.983 CFI=.987, RMSEA=.055, SRMR= .029 and HOELTER (210) (see Table 7-56).

Table 7-56: The successful ICT risk management (SICTRM) model in SEM

Cut-off Value		Model Fit	Cut-off Value		Model Fit
Indices	Required Value		Indices	Required Value	
χ^2/df (113.762/60)	< 3	1.896	RMSEA	< .06	.055
P-value	> .05	.251	SRMR	< .08	.029
TLI	≥ .90	.983	HOELTER		
CFI	≥ .90	.987	P=0.05	≥ 200	210

All indices met the requirements, suggesting that the structural model explains the data well. Moreover, the squared multiple correlations (R^2) for the structural model, which represent the amount of variance in each endogenous variable predicted by exogenous variables, were estimated. The R^2 of the enterprise information security plan (ESP) is .77, which indicates that one exogenous variable (organisational policy-POLICY) and one endogenous variable (management of ICT resources-IT) explained 77% of the variance in the ESP (see Figure 7-39). Likewise, the R^2 of the model was .47, which indicates that three latent variables (organisational policy-POLICY, management of ICT resources-ICT and the enterprise information security plan-ESP) explained 47% of the variance in successful ICT risk management (SICTRM). However, 53% of unexplained variance in the successful ICT risk management (SICTRM) model is also considered in terms of the optimisation of the model. Unexplained variances might result from the types of sample adopted in the qualitative and quantitative methods. The types of sample in the qualitative method include the banking and software development sectors, which may affect the validation in the quantitative method. For example, both the banking and software development sectors might consider service management as other success factors, related to other standards (i.e. the ITIL framework and the Basel II accord), when dealing with ICT risk management (ITGI 2007; Basel 2005).

The estimation values of the structural model are χ^2=113.762, df=60, χ^2/df=1.896 and p=0.251. These measures indicate that the structural model has a good fit, which then leads to the initial model grounded on the qualitative findings being rejected, as supported by the research of Bentler and Bonett (1980). This researcher therefore proposes that the success factors for ICT risk management in an organisation are more likely to be organisational policy (POLICY), management of ICT resources (IT), and the enterprise level plan (ESP). Three success factors were therefore validated in the SEM in order to confirm the relationship and significance among the factors for establishing successful ICT risk management in an organisation.

SEM was further utilised along with maximum likelihood estimation (MLE) and bootstrapping (due to the small sample size and to boost accurate data) to further analyse the data. In bootstrapping, both the biased-corrected p-value and the percentile p-value were used with a 95% confidence level, as recommended by Byrne (2001), to ensure that results would not occur by chance.

The two p-values for the relationships between organisational policy (POLICY) and the enterprise information security plan (ESP) to establish successful ICT risk management (SICTRM) are 0.002 (p_{bc}) and 0.004 (p_{pc}) respectively (see Table 7-57). It can therefore be argued that organisational policy has a positive effect (.441) on the enterprise information security plan (ESP) in establishing successful ICT risk management (see Table 7-58). Furthermore, organisational policy (POLICY) has an indirect effect (0.323)

through management of ICT resources (IT) on the enterprise information security plan (ESP) (see Table 7-58) with the p-values of 0.000 (p_{bc}) and 0.000 (p_{pc}) respectively (see Table 7-59).

An indirect effect implies that organisational policy is driven to the operational level to effectively plan enterprise information security in order to achieve successful ICT risk management (Stoneburner et al. 2002). As a result, it supported the theoretical concept of strategic management (Wheelen & Hunger 2004). Organisational policy was defined at the board of director (the strategic level) and then was driven to the senior management and operational levels (the management level) in order to plan information security control together to achieve successful ICT risk management.

To apply this latent variable (POLICY), information security (IS) objectives must be clearly defined in dealing with ICT risk management. In addition, it is necessary to formulate a risk statement to scope information security definitions so that Thai business organisations focus on the policy regarding information security management. These relationships then indicate that Thai organisations delineate organisational policy in terms of an enterprise information security plan (ESP) in IS strategy within their policy statements. This approach will enable an organisation to achieve its goals in dealing with ICT risks in both directions.

Table 7-57: Standardised regression weights: P-values at a 95% confidence interval

Parameter			p_{bc}	p_{pc}
IT	<---	POLICY	.004	.004
ESP	<---	IT	.006	.004
ESP	<---	POLICY	.002	.004
SICTRM	<---	ESP	.026	.024
SICTRM	<---	IT	.004	.005

Table 7-58: Standardised effects of successful ICT risk management

	POLICY			IT			ESP		
	Direct	Indirect	Total	Direct	Indirect	Total	Direct	Indirect	Total
IT	.604	-	.604	-	-	-	-	-	-
ESP	.441	.323	.764	.535	-	.535	-	-	-
SICTRM	.000	.496	.496	.354	.197	.552	.369	-	.369

Table 7-59: Standardised indirect effects: P-values at a 95% confidence interval

	p_{bc}				p_{pc}			
	POLICY	IT	ESP	SICTRM	POLICY	IT	ESP	SICTRM
IT	...	...	...	...	...	...	...	...
ESP	.000	...	...	...	.000	...	...	...
SICTRM	.000	.018	...	...	.000	.015	...	...

The two p-values for the relationships between organisational policy (POLICY) and management of ICT resources (IT) to establish the enterprise information security plan

(ESP) and successful ICT risk management (SICTRM) are 0.004 (p_{bc}) and 0.004 (p_{pc}) respectively (see Table 7-57). It can be argued then that organisational policy has a positive effect (.604) on the management of ICT resources in establishing the enterprise information security plan and successful ICT risk management (see Table 7-58). Moreover, organisational policy also has an indirect effect (.496) through the management of ICT resources and the enterprise information security plan on successful ICT risk management (see Table 7-58) with p-values of 0.000 (p_{bc}) and 0.000 (p_{pc}) respectively (see Table 7-59).

An indirect effect implies that organisational policy is driven to the operational level to effectively manage ICT resources and to effectively plan enterprise information security in order to achieve successful ICT risk management (Stoneburner et al. 2002). As a result, this indirect effect supported the theoretical concept of strategic management (Wheelen & Hunger 2004). Organisational policy was defined at the board of director (the strategic level) and then was driven to the senior management and operational levels (the management level) in order to plan information security control together to achieve successful ICT risk management.

To apply this latent variable (organisational policy), information and communication technology objectives must be clearly defined in dealing with ICT risk management. In addition, it is necessary to formulate a risk statement to scope ICT resources definitions so that Thai organisations focus on the policy regarding the management of ICT resources. These relationships then indicate that Thai organisations should delineate ICT strategy as ICT objectives within their policy statements. This approach will enable Thai organisations to better achieve their goals when dealing with ICT risks in both directions.

The two p-values for the relationships between management of ICT resources (IT) and the enterprise information security plan (ESP) to establish successful ICT risk management (SICTRM) are 0.006 (p_{bc}) and 0.004 (p_{pc}) respectively (see Table 7-57). This indicates that the management of ICT resources has a positive effect (0.535) on the enterprise information security plan in achieving successful ICT risk management (see Table 7-58). When reflecting on the management of ICT resources, Thai organisations appear to ensure that the same data and information patterns are considered when planning ICT risk management. Software licensing or applications with licensing can also assist Thai organisations to mitigate, prevent and avoid ICT risks. These relationships show that the management of ICT resources and information security are distinct from each other. The management of ICT resources focuses on providing ICT facilities to all staff in Thai organisations. In contrast, the enterprise information security plan focuses on information security control and audit instead.

The relationships between the management of ICT resources (IT) and successful ICT risk management (SICTRM) are revealed by the p-values of 0.004 (p_{bc}) and 0.005 (p_{pc}) respectively (see Table 7-57). This signifies that the management of ICT resources has a positive effect (0.354) on successful ICT risk management in organisations (see Table 7-58). Furthermore, the management of ICT resources also has an indirect effect (0.197) through the enterprise information security plan on successful ICT risk management (see Table 7-58) with p-values of 0.018 (p_{bc}) and 0.015 (p_{pc}) respectively (see Table 7-59).

An indirect effect implies that enterprise information security plan helps the effective management of ICT resources improve successful ICT risk management. The indirect effect was supported by the theoretical concept of information security management (Stoneburner et al. 2002). Managing ICT resources with information security control can help achieve the mitigation, the avoidance and the prevention of ICT risks.

This indicates that the management of ICT resources (i.e. sufficient networking connection, maintaining the same data and information patterns, and software licensing or applications with licensing) is significant for enabling Thai organisations to mitigate, prevent and avoid ICT risks. Thus, focusing only on the management of ICT resources, an organisation can achieve successful ICT risk management.

Lastly, the relationships between the enterprise information security plan (ESP) and successful ICT risk management (SICTRM) are revealed by the p-values of 0.026 (p_{bc}) and 0.024 (p_{pc}) respectively (see Table 7-57). This signifies that the enterprise information security plan has a positive effect (0.369) on successful ICT risk management in organisations (see Table 7-58), although this factor is generated from the combination of human resource management and planning, organisational security, corporate level planning and operational level planning. However, this does not mean that the indicators among the four factors are similar in content, but they are in structure. In other words, all indicators are considered as one factor by combining two plans (at the corporate and the operational levels) into one plan, as per organisation theory (Christensen et al. 2007). Furthermore, this combination of four factors is supported by the suggestion of Solms (2005a), who claims that information security governance as in the ISO/IEC 17799 standard (including human resources protection and management, and organisational security) needs to be considered at both the corporate and the operational levels. Consequently, the enterprise information security plan plays a vital role in successfully dealing with ICT risk management.

7.12 Conclusion

The quantitative results were scrutinised to demonstrate the survey analysis. The survey analysis carefully examined the data in detail, utilising descriptive statistics, reliability, coefficient values, univariate and multivariate normality tests, content validity, convergent validity, discriminant validity and nomological validity, in order to ensure that the data conformed to the requirements of EFA, CFA and SEM. Furthermore, non-normal data distribution did not affect the analysis, although the data in this research are not normally distributed. The reason was because this research used bootstrapping to deal with inaccurate results statistically estimated from non-normal data distribution. This resampling technique allows the researcher to test the model under conditions of multivariate normal distribution accurate results can be obtained (Byrne 2001).

The survey analysis started with the demographic statistics of the sample. This survey included three types of business (banking, telecommunications and insurance). The number of respondents was 302 from the 1,000 survey questionnaires sent out. This is equal to a 30.20% response rate. Once analysing the demographic statistics, data cleaning was undertaken to reduce the number of indicators. The rationale for this is because the ratio of sample size to the number of free parameters should be at least 5:1 to obtain trustworthy parameter estimates and at least 10:1 to obtain appropriate significance tests.

The questions in the survey were produced using the proposed indicators as key elements formulated in Chapter 6. In particular, the indicators in Human resource management and Planning (HRMP), and Organisational Information Security (OS) were expanded into several questions in order to facilitate better understanding of the question/item and indicators. Therefore, they had to be reduced to meet the original indicators grounded in the proposed dimensions from Chapter 6 (HRMP on p. 154 and OS on p. 156). By doing so, the ratio of sample size to the number of free parameters was not only met but also the original indicators were maintained. To undertake this process, item parcelling was performed to reduce the number of indicators by using their average means to represent the new mean for the new indicator (the original indicator grounded in the proposed dimensions). Each dimension is then ready for validation in the eight stages of the quantitative analysis. Each stage is discussed next.

Stage I

Each indicator in the survey was firstly validated for its significance by using the Chi-square test in SPSS. After screening the data, all indicators and dimensions were shown to be significant and ready for validation in the next stage.

Stage II

Reliability testing was used to evaluate the internal consistency of the scale that measures the reliability of instrument stability. This reliability testing was Cronbach's Alpha performed in SPSS. The results show that the Cronbach's Alpha coefficient scores ranged from 0.904 to 0.942 across the factors, which are greater than 0.6 for exploratory research. Therefore, the results demonstrate good reliability of internal consistency. The data was then ready to validate in the next stage.

Stage III

Conceptual model validation was used to evaluate the model generated from the qualitative analysis. This validation was conducted using structural equation modelling in combination with consideration of the factor loadings, the p-values and the critical ratio (CR), the modification indices (MI) and the goodness-of-fit (GOF) values. As a result, the conceptual model based on the qualitative analysis was rejected on the basis of several problematic issues such as the insignificance of each path, the insignificance of the model and the low factor loadings. The conceptual model was then rectified to develop the model using SEM. The next stage involved the processes of validation in SEM.

Stage IV

Validity testing and model analysis involved content and construct validity tests. Prior to launching the survey, the questionnaire was pilot-tested to validate content validity. Two researchers were engaged to validate the items to ensure that sense and meaning were clearly represented. Ten experts were also engaged to confirm the contents where the clarity of meaning needed improvement. Once sense, meaning and the clarity of meaning were achieved, construct validity testing was undertaken.

In this regards, this research followed a four-step modelling process based on Mulaik and Millsap's (2000) approach to performing construct validity. Construct validity based on the tests of convergent validity, discriminant validity and nomological validity was used to confirm that the indicators align with the factors in multiple processes of measuring instrument adequacy. Construct validity started with convergent validity by using confirmatory factor analysis (CFA) in the next stage.

Stage V

Confirmatory factor analysis (CFA) was used to estimate the value of the factor loadings between the indicators and the factor. The factor loading indicates the correlation between the indicators and the factor. Maximum likelihood (ML) and bootstrapping were used in conjunction with CFA because this survey has a small sample size. ML helps deal with a small sample size but is good for dealing with multivariate normally distributed data. However, the data in this research were not multivariate normally distributed.

Therefore, bootstrapping was used to boost the accuracy of values from the ML estimator (MLE). MLE used together with the bootstrapping technique in CFA provides p-values with a Bollen-Stine bootstrap to test the significance by obtaining the χ^2 value for the model and the indicators.

Before undertaking CFA validation, the researcher set up four processes for rectifying the model, and provided the following guidelines for model modification to ensure any changes were appropriately scrutinised:

- Factor loadings must be greater than 0.7; otherwise they will be dropped.
- The p-value of each item or observed variable must be less than 0.05; otherwise it will be deleted.
- Modification indices were considered to rectify and delete any problematic issues after careful consideration, if there are the highest covariance values between indicators which mean that both indicators relate to misspecification.
- Goodness-of-fit (GOF) cut-off values were set at χ^2/df<3 and p-value>.05 (the model); CFI and TLI ≥.95; SRMR <.08; RMSEA <.06; and HOELTER ≥200, which represent a good model fit. Moreover, if the critical ratio of kurtosis value generated in AMOS is greater than 1.96 this means that the data do not display multivariate normal distribution. In this case, the bootstrapping technique is undertaken with ML at every stage of the ongoing process of model modification.

After validating the indicators and the dimensions through CFA, one indicator (os6−physical protection) in the organisational information security (OS) dimension was dropped for having a low factor loading (0.66). Another indicator (os1−system configuration) in the same dimension was duplicated with two other indicators (it1−providing sufficient networking connection and it2−providing personnel computers) in the management of ICT resources (IT) dimension. Therefore, the results of factor loadings for all indicators were greater than 0.7, except for the indicator (clp1−the managerial view) for the corporate level plan (CLP) and the indicator (olp1-the operational view) for the operational level plan (OLP). However, both indicators did not affect the model fit in each dimension; therefore, it is acceptable that they remain in each dimension. Once convergent validity was met, discriminant validity testing was next undertaken.

Stage VI

Discriminant validity was used to evaluate the difference among dimensions in the model. This test ensures that each dimension is unidimensional such that each dimension in the model represents a different construct but in the same direction. Therefore, the

values of correlation between factors should be less than .85. In addition, the average variance extracted (AVE) for two dimensions must be greater than the square of the correlation between the dimensions in order to satisfy the requirements of discriminant validity.

Testing for discriminant validity revealed that there were three pairs of dimensions that did not hold discriminant validity. The first pair included human resource management and planning (HRMP) and organisational information security (OS). The results suggested that these dimensions should be combined as one dimension, renamed as organisational security management (OSM). The second pair included the corporate level plan (CLP) and the operational level plan (OLP), for which it was statistically suggested that they also be combined into one dimension, which was renamed the enterprise level plan (ELP). The last pair included organisational security management (OSM) and the enterprise level plan (ELP), which similarly were combined into one dimension, the enterprise information security plan (ESP).

Exploratory factor analysis (EFA) was first used to confirm whether or not both dimensions represented content similarity and/or structural similarity. Once the first method was performed, CFA was repeated to reconfirm the results, and drop the insignificant indicator in the new construct by following the four processes for rectifying the model, until all dimensions were found to hold discriminant validity. The measurement model or dimension validity is discussed in the following.

Stage VII

The measurement model or dimension validity was used to determine the reliability of the instrument along with its indicators. In so doing, all factors along with their indicators were statistically analysed by determining that: (1) the factor loadings must be greater than 0.7; (2) the standardised residuals must be less than 2.5; and (3) the critical ratio must be greater than 1.96. As a result, these three criteria were met, and the following three indicators were discarded, thereby resolving the problematic issue in the modification indices (MI):

- policy4 (Business Continuity Plan) in the Organisational Policy dimension;
- esp1 (IS in security direction) in the Enterprise Information Security Plan dimension; and
- it2 (providing sufficient personal computer) in the Management of ICT Resources dimension.

As a result, the latent dimensions account for more than 68% of the variance in each of the indicators; thus, they are good measures of the dimensions. In other words, four

dimensions out of the original seven explored in the qualitative analysis were confirmed as indicators of success to establish ICT risk management. The next stage is the final stage of the quantitative analysis.

Stage VIII

Structural equation modelling (SEM) was used to show that the four factors derived from stages VI and VII represented relevant dimensions. The structural model indicates that organisational policy has the greatest impact on the management of ICT resources and the enterprise information security plan to establish successful ICT risk management. In this regard, the impact of organisational policy on the management of ICT resources and the enterprise information security plan is supported by the theoretical concepts of strategic management in organisations (Wheelen & Hunger 2004). The results of SEM reveal that the R^2 of the model is 0.47 (see Figure 7-40), which indicates that organisational policy (POLICY), management of ICT resources (IT) and the enterprise information security plan (ESP) explained 47% of the variance in successful ICT risk management (SICTRM).

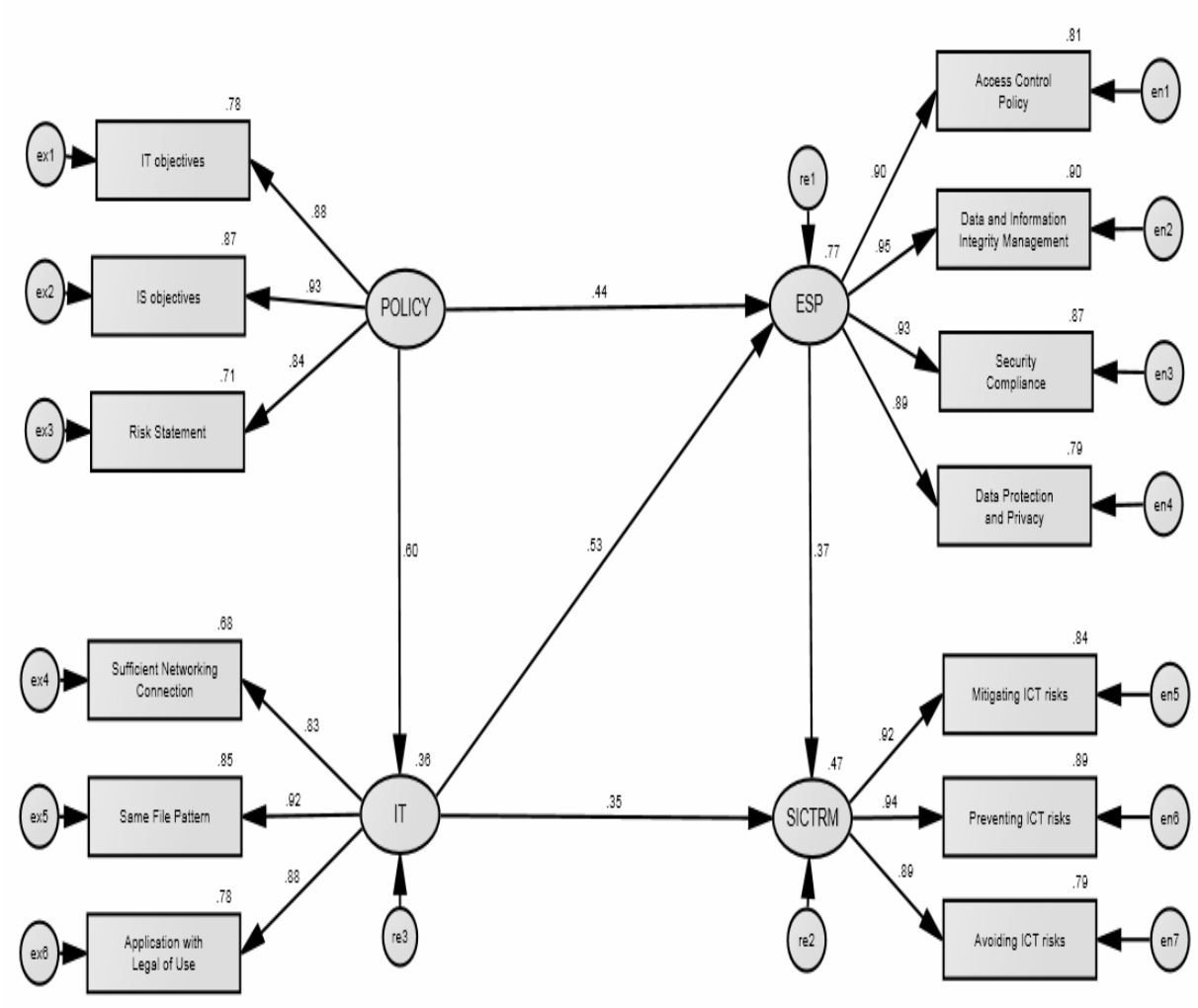


Figure 7-40: The structural model of successful ICT risk management (repeated from Figure 7-39)

However, 53% of unexplained variance in the successful ICT risk management (SICTRM) model might result from the types of sample used in the qualitative and quantitative methods. The types of sample included the banking and software development sectors, which might consider service management as a success factor, related to other standards (i.e. the ITIL framework and the Basel II accord) when dealing with ICT risk management (ITGI 2007; Basel 2005).

At each stage of the SEM analysis, CFA was performed carefully to maintain the reliability and validity of the data, during construct validity testing in particular. The errors and biases in the model were also minimised during the eight stages. As a result, three success factors for dealing with ICT risk management in Thai business organisations were identified. Organisational policy, the management of ICT resources and the enterprise information security plan (combined with organisational security, human resource management and planning, the corporate level plan and the operational level plan) were confirmed to drive successful ICT risk management planning. The next chapter will discuss the contributions and the conclusions of this research.

Chapter 8

DISCUSSION AND CONCLUSION

This chapter discusses the major findings of the research and concludes with consideration of its implications. The research limitations and suggestions for future research are also discussed in the final section of this chapter.

The purpose of this research was to understand success factors for ICT risk management practices in Thai business organisations. The research objectives of this research were:

- To investigate the current profile of ICT risk management in organisational practices in a sample of Thai businesses,
- To identify and then model the success elements of ICT risk management in Thai businesses.

The research question developed from these objectives was:

- What factors determine successful ICT risk management in a business organisation in the Thai business context?

Three subsidiary questions are developed to support this major question, as follows:

- What are the current profiles of ICT risk management in Thai businesses?
- How are ICT risk management concepts applied in those Thai businesses? and,
- What success factors can be identified for successful ICT risk management derived from the adoption of the COBIT framework and the ISO/IEC 17799 standard?

8.1 Success factors in ICT Risk Management in Thai Business

This research achieved validation of the nature of the success factors in Thai business by comparing ICT risk management in practice with the COBIT framework and the ISO/IEC 17799 standard to propose one single management framework for dealing with operational, technical and strategic risk related to ICT. Moreover, this research supported the conclusions of Solms (2005b), that integrating control processes of the COBIT framework and the ISO/IEC 17799 standard work best through a two-way approach to ICT risk management. While the COBIT framework lays the foundation of a top-down approach to risk management, the ISO/IEC 17799 standard supports a bottom-up

approach. The three success factors shown in this study, creating organisational policy (drawn from both the COBIT framework and the ISO/IEC 17799 standard), managing reliable ICT resources (drawn from the COBIT framework), and effectively planning enterprise information security (drawn from both the COBIT framework and the ISO/IEC 17799 standard), were found to positively contribute to successful ICT risk management. It was found that three success factors were commonly accepted as vital for successful ICT risk management in Thai business organisations.

This study of ICT risk management in Thai organisations revealed that the development of organisational structure, organisational process, organisational control and organisational ICT strategies were considered essential to deal with ICT risk management. Firstly, the Thai business organisations clarified their organisational structure in determining the roles and responsibilities of employees in all staff levels, developed organisational policies about the objectives of their use of ICT and information systems, and introduced a culture of ICT risk management treatment and the components of ICT risk management processes. Secondly, the Thai business organisations developed their organisational processes to deal with ICT risks through the development of ICT risk management instruments and the processes of ICT risk management. Thirdly, the Thai business organisations controlled people, processes, technology and systems simultaneously in order to prevent, avoid and mitigate operational, technical and strategic risks related to ICT, as both a proactive and a reactive process. Lastly, their ICT risk management strategy entailed collaboration between senior management and operational level staff aimed at establishing both corporate and operational plans for dealing successfully with ICT risk.

Success factors derived from the control processes in the COBIT framework and the ISO/IEC 17799 standard were identified in the processes adopted in the Thai organisations.

The outcomes of this research revealed that the effective creation of organisational policy, the effective management of ICT resources and the effective planning of enterprise information security were the key success factors positively affecting successful ICT risk management in Thai organisations. These conclusions are outlined in Table 8-1 comparing the findings with existing research about ICT risk management success:

Table 8-1: Summary of the research findings

Results of this study	Comparison to previous studies
Organisational policy The results from multiple case studies have shown that organisational policy used in the Thai organisations for ICT risk management consisted of a combination of ICT policy, information security policy, a risk statement and a statement about business continuity management. The results from the survey confirmed that the effective creation of organisational policy required creating ICT policy, creating ICT security policy and documenting organisational policy in a risk statement. This was shown to have a positive direct effect on effective management of ICT resources (POLICY→ICT=.604, p≤0.05) and the effective planning of enterprise information security (POLICY→ESP=.441, p≤0.05) as well as an indirect effect on the effective planning of enterprise information security (POLICY→ESP=.323, p≤0.05) and successful ICT risk management (POLICY→SICTRM=.496 p≤0.05). This study concluded that the effective creation of organisational policy was a key success factor for developing an ICT risk management plan to mitigate, avoid and prevent operational, technical and strategic risks related to ICT in Thai businesses.	From both results, this research revealed that effective organisational policy was required to create ICT, security and business directions to direct the effective planning of enterprise information security and the effective management of ICT resources for succeeding an ICT risk management plan. These results were consistent with the previous research of Badenhorst and Eloff (1994), Benaroach et al. (2006), Bojanc and Jerman-Blažič (2008), Buckby et al. (2009), Iijima and Curtis (2004), McEvoy and Whitcombe (2002), Smith and Eloff (2002), Straub et al (2008) and Straub and Welke (1998). They suggested that ICT policy, ICT security policy and documentation of policy were considered when creating organisational policy in organisations to deal with strategic risks related to ICT.
Management of ICT resources The results from this research have shown that the process of managing ICT resources in Thai businesses consisted of a number of actions: the configuration of networking and personal computers; software licensing; and managing data and information patterns. The research confirmed that the effective management of ICT resources required providing sufficient networking connection, providing proper or complete software licence, and managing database systems. These actions were shown to have a positive direct effect on the effective planning of enterprise information security (ICT→ESP=.535, p≤0.05) and successful ICT risk management (ICT→SICTRM=.354, p≤0.05) as well as an indirect effect on successful ICT risk management (ICT→SICTRM=.197, p≤0.05). This study concluded that managing reliable ICT resources	This study confirmed the study results of Byrd et al. (1995), Coles & Moulton (2003), Flowerday & Solms 2005, Hermanson et al. (2000), Longstaff et al. (2000), Moeller 2005, Saint-Germain (2005), Smith & Eloff 2002, Straub and Welke (1998) and Theoharidou et al (2005). They argued that maintaining data and information integrity helped organisations deal with operational risk in ICT risk management. In addition, this study also supported the assertions of Luftman et al. (1993), McLeod and Schell (2007), McNurlin and Sprague (2006), O'Brien and Marakas (2009), and Whitman and Mattord (2009). They argued that the provision of adequate technology and facilities enable the processing of software and workflow

helped maintain data and information integrity. In addition, this research showed that the effective management of ICT resources affected the effective planning of enterprise information security for establishing successful ICT risk management plans.	applications through the ICT infrastructure in order to achieve successful ICT risk management.
The enterprise security plan The results from this research have demonstrated that managing people and their behaviour in the Thai organisations consisted of a number of actions: understanding and clarifying the control roles and responsibilities of staff, protecting information security from inappropriate behaviour of staff, securing information security from inappropriate behaviour of staff and providing training and education programs for staff. Managing information security in ICT infrastructure in the Thai businesses was shown to relate to protecting physical and logical access control, managing data and information integrity, applying security rules and complying with regulations and laws, both internal and external to the organisation, and protecting data and privacy. Planning ICT risk management at the Thai corporate level consisted of actions such as defining ICT control and audit, defining ICT processes to cover overall ICT functions fitting with ICT policy, and providing overall ICT risk management process. Planning ICT risk management at the operational level was shown to deal with defining information security (IS) control and audit, defining IS processes to technical functions fitting with information security policy and providing specific ICT project risk management process for each project or for each department in the organisation. The results from the research have showed that four of the key factors relating to ICT risk management success, that emerged from the case studies, merged into one key factors statistically, the effective planning of enterprise information security. This success factor was shown to require organisations to manage and document access control policy, manage data and information integrity, comply with enterprise information security rules and regulation, both internal and external, and protect data and privacy. The analysis of the data showed that the factor effective planning of enterprise information security had a positive and direct effect on successful ICT risk management (ESP→SICTRM=.369, p≤0.05).	This research confirmed the conclusions of Allen (2005), Buchanan & Gibb (2007), Caralli et al. (2004), Capuder (2004), Eloff and Eloff (2003), Grove (2003), Jordan and Silcock (2005), Robinson (2005), Mena (2002) and Solms (2005a). They argued that an information security plan needed to be the focus at both the corporate level and the operational level together in the creation of an the enterprise-wide plan. In addition, Mena (2002) further argued that the close cooperation between senior management and the operational team was able to attain the optimal goals in ICT risk management. This study extended the work of Solms (2005a) that in that study it showed that the information security plan needed in the Thai organisations was a dual policy, set first at the enterprise and then at the organisational level.

8.1.1 Organisational policy

The results of the analysis of data from the case studies showed that the Thai organisations identified two key ICT risk elements that needed to be addressed for success in their management of ICT risk, one related to information and communication technology (ICT) risk and the other to information security (IS) risk. The ICT risk emerged from poor ICT risk management processes in various departments in each of the case studies. The case studies revealed that ICT risk resulted from uncontrolled practices including the use of pirated applications and software, from improper or incomplete software licence, from poor protection of intellectual property and from incomplete software maintenance and updating. On the other hand, the case studies showed that IS risk, related to technical security, resulted from poorly managed or constructed databases, poorly managed servers, old operating systems, poor networking management and maintenance, poor setting configurations and penetration testing breaches. The case studies revealed that the objective of each organisation in managing technology for risk was to define the appropriate control mechanisms for management of existing ICT resources and of information security, which related, they revealed, to having a complete understanding of people, processes, technology and systems in their organisation. The respondents in the case studies said that their objective was to control the processes, technology and systems appropriately by delegating the responsibilities to people within their organisations in order to achieve business objectives and goals. The Thai organisations objectives were to focus on security issues that involved developing a systematic process to protect organisational technology and systems from a variety of problems related to operational, strategic and technical risks of corporate data loss, or business continuity. To achieve this, the Thai organisations all noted that ICT and IS objectives were best addressed by adoption of and clarity in various organisational policies.

The findings from previous research (Badenhorst and Eloff 1994; McEvoy and Whitcombe 2002; Bojance and Jerman-Blažič 2008; Smith and Eloff 2002; and Iijima and Curtis 2004) showed that when dealing with ICT risk management, information technology and information security policies needed to be defined separately by setting information technology and information security objectives to direct information technology policy and information security policy respectively. The data collected from the case studies in Thailand supported this conclusion that the setting of information technology objectives were built into information technology policy and information security objectives were built into information security policy. These policies were used in the Thai organisations to deal with ICT risk management.

The respondents in the case studies mentioned that an organisational policy for ICT risk management had to deal with risk definition, the responsibility for risk management at all

management levels, outline a risk management methodology, determine and make explicit, risk control and auditable areas. The policy statement (i.e. a risk statement) in the Thai interviews was most often derived from their adoption of either or both COBIT framework and the ISO/IEC 17799 standard. This practice confirmed the determinations of the COBIT framework that an organisational policy document must exist for successful ICT risk management and provide the general and specific responsibilities for ICT risk management and be related to the organisation's business (ITGI 2007; ISO/IEC 2005). The respondents in the case studies noted that the organisational policies for ICT risk management needed to be communicated to staff and that staff roles and responsibilities were clear when risks occurred. These practices align with the determinations in both COBIT and the ISO/IEC 17799 standard (ITGI 2007; ISO/IEC 2005).

In the Thai case studies, business continuity planning was also considered as a key element of organisational policy in each company to maintain a contingency plan for successfully dealing with strategic, operational and technical risks in the organisation. The focus on the business continuity plans in the Thai interviews confirmed the work of Calderson and Dishovska (2005) and Cha et al. (2008), that for successful ICT risk management technology planning, security assessment, risk statements and business continuity plans need to be incorporated in organisational policy, and that these positively affect planning at both the corporate level and the operational level when undertaking ICT risk management.

Creating both an ICT policy and information security policy were confirmed in the survey analysis as being key indicators of success in ICT risk management (Chapter 7, p. 231). Creating ICT and IS policies were shown to be significant indicators because clear ICT and IS directions are required to define and then manage ICT risks at the senior management level. By creating both policies, the organisation can determine a clear direction of dealing with ICT risk management. The organisational policy enabled the organisation to clarify both ICT and IS objectives, and was the key indicator of success in the organisational policy, to cover both management of ICT resources and management of information security simultaneously, when the organisation was planning to deal with ICT risk management. From this point of view, the planning and organising of ICT was showed in this research to enable Thai organisations to follow the control objectives of defining a strategic ICT plan, determining a technological direction and ensuring continuous services in the same way it was defined in COBIT (ITGI 2007).

The document of organisational policy (i.e. the risk statement) was confirmed in the survey analysis (Chapter 7, p. 231) as another indicator of success from the determinations in organisational policy. Policy was identified in the Thai organisations as essential to direct the risk management processes in each organisation. The document

of organisational policy was used to outline a brief risk definition, the responsibility for risk management, risk management methodology, risk control and auditable areas. The focus of the document of organisational policy in Thai organisations was to ensure that ICT risk management was clear at all staff levels in order to perform organisational planning appropriately at both the corporate and the operational levels in ways similar to that prescribed in the ISO/IEC 17799 standard (ISO/IEC 2005). Only business continuity planning was showed to be insignificant as an indicator of successful ICT risk management relating to the use of organisational policy.

Organisational policy in the Thai businesses studied required senior management to create a document of both ICT and IS policies to enable them to achieve successful ICT risk management (Table 8-2). Creating organisational policy was showed in both parts of this research to be a clear success factor for establishing successful ICT risk management in Thai businesses. The statistical results in this research revealed that organisational policy was a significant factor for successful ICT risk management. This research also showed that the relationships between organisational policy and the enterprise security plan were significant to establish successful ICT risk management with both the biased-corrected p-value ($0.003-p_{bc}$) and the percentile p-value ($0.004-p_{pc}$) at a 95% confidence level. Moreover, this research also showed that the relationships between organisational policy and management of ICT resources ware also significant to establish the enterprise security plan and successful ICT risk management with both the biased-corrected p-value ($0.004-p_{bc}$) and the percentile p-value ($0.004-p_{pc}$) at a 95% confidence level.

Table 8-2: Organisational policy

Parameter		λ	R^2	P-value	Significance
Factor	Indicator				
Organisational policy	ICT policy	.885	.783	***	Yes
	Information security policy	.933	.871	***	Yes
	A risk statement	.843	.711	***	Yes

Furthermore, the survey also revealed that the effective creation of organisational policy has an indirect effect (.496) through the effective management of ICT resources and the effective planning of enterprise information security, on successful ICT risk management with both the biased-corrected p-value ($0.000-p_{bc}$) and the percentile p-value ($0.000-p_{pc}$) at a 95% confidence level. In addition, the survey revealed that the effective creation of organisational policy has an indirect effect (.323) through the effective management of ICT resources on the effective planning of enterprise information security with both the biased-corrected p-value ($0.000-p_{bc}$) and the percentile p-value ($0.000-p_{pc}$) at a 95% confidence level. Both indirect effects imply that the effective creation of organisational policy at the senior management level requires the operational

managers to control ICT resources and to plan enterprise information security in order to achieve successful ICT risk management, confirming the previous conclusion of (Stoneburner et al. 2002). The effects of the adoption and implementation of clear organisational policy on ICT risk was shown then to be a clear indicator of ICT risk management success in Thai business organisations.

8.1.2 Management of ICT resources

The results of the analysis of data from the case studies showed that the implementation of control mechanisms to maintain data and information integrity were the focus to manage ICT resources in organisations. Control mechanisms were implemented to manage ICT resources which were a key factor that they identified affected control planning at both the corporate and operational levels in successful ICT risk management. The respondents in the case studies argued that ICT resources had to be managed properly in order to meet each organisation's ICT objectives and ensure avoidance of operational risk. They also revealed that managing proper licence and proprietary of ICT resources was necessary for successful ICT risk management. This included secure management of facilities, networking, personal computers, database management systems and software. The respondents in the case studies argued that ICT control and audit plan was used to manage ICT resources in order to maintain data and information integrity including effectiveness, efficiency, confidentiality, integrity, availability and reliability of data and information. Most respondents recognised that this was undertaken seriously in their organisations. ICT control and audit plan are use in these organisations to identify and maintain reliable ICT infrastructure. Reliable ICT infrastructure they defined as the requirement of having sufficient networking connection, having efficient database systems, and providing proper or complete software and applications licence. The respondents in the case studies believed that management of reliable ICT resources directly affected successful ICT risk management. The findings from previous research of Luftman et al. (1993); McLeod and Schell (2007); McNurlin and Sprague (2002); O'Brien and Marakas (2006); and Whitman and Mattord (2009) showed that management of reliable ICT resources enabled organisations to prevent, avoid and mitigate operational risk. As a result, it was seen in the case studies that the effective management of ICT resources required providing sufficient networking connection, managing database system, and providing proper or complete software licence to avoid, mitigate and prevent operational risk in ICT risk management.

Providing sufficient networking connection was argued as the key factor that determined effective management of ICT resources in the case studies. The respondents suggested that effective management of the network connections derived from providing sufficient

networking connection to all staff in order to facilitate automated business applications. Their organisations were able to ensure that data and information processed in reliable ICT resources maintained data and information integrity in order to avoid, prevent and mitigate operational risks. Providing sufficient networking connection was then confirmed in the survey analysis (Chapter 7, p. 233) as a key indicator of the effective management of ICT resources. The reason was that providing sufficient networking enabled the processing of software and workflow applications through the ICT infrastructure in order to achieve successful ICT risk management.

The respondents in the case studies also argued that database systems management affected maintaining data and information integrity. Database systems management was required to effectively managing ICT resources, and they believed, that influenced successful ICT risk management. The reason given was that operational risks related to ICT can be mitigated, avoided and prevented by their adoption. The findings from the previous research of Ousterhout et al. (1985) and Straub and Welke (1998) had showed that managing database systems helped organisations maintain data and information integrity to achieve the effective management of ICT resources. The indicator, managing database systems, was then confirmed as having an impact on the effective management of ICT resources in the survey analysis (Chapter 7, p. 233). The reason given by the interviewees was that database systems management enabled maintaining data and information integrity while effectively managing ICT resources to achieve successful ICT risk management.

The respondents in the case studies revealed that software licence was a major concern among Thai business organisations. Providing proper or complete software licensing was also a concern of the respondents in the case studies as they believed that it had an important influence on their effective management of ICT resources. They noted that software piracy caused obstruction of their commercial licence agreements which led to operational risk directly affecting successful ICT risk management in their organisations.. Risk management in the Thai organisations related not only to software used in the organisation but also to software installed on the personal computers of staff, both of which impacted on the ICT operations in their organisations. Lloyds (2000) argued in previous research that all intellectual property must be used under property rights. In addition, Rife (1994, p. 364) mentioned that software piracy 'is the single greatest threat to the continued success of the industry'. Rife (1994, p. 364) further added that 'the piracy rate in Thailand (where there is no effective copyright protection for software) is estimated to be 99%'. The Thai business organisations have now started to become more concerned about software licensing. Since 2007 the Royal Thai Government has passed a new law on computer-related offences, the *Computer Crimes Act*, which all Thai business organisations are forced to follow (AHRC 2007). The case studies highlighted the

importance of managing software licensing as integral to ICT risk management. Providing proper or complete software licensing was also then confirmed as a determinant of effective management of ICT resources in the survey analysis (Chapter 7, p. 233). The reason given by the interviewees was that providing proper or complete software licensing enabled their organisations to avoid operational risk emerging from software piracy.

The effective management of ICT resources in the Thai businesses studied required providing sufficient networking connection, effectively managing database systems and providing proper or complete software licensing to achieve successful ICT risk management (Table 8-3). The effective management of ICT resources was showed in both part of the research to be a clear indicator of success for achieving successful ICT risk management in the Thai business organisations. The statistical analysis results showed that the management of ICT resources was a significant factor for successful ICT risk management. This research also showed that the relationships between the effective management of ICT resources and effective planning of enterprise information security were significant to establish successful ICT risk management with both the biased-corrected p-value ($0.006-p_{bc}$) and the percentile p-value ($0.004-p_{pc}$) at a 95% confidence level. Moreover, the effective management of ICT resources directly affected successful ICT risk management with both the biased-corrected p-value ($0.004-p_{bc}$) and the percentile p-value ($0.005-p_{pc}$) at a 95% confidence level.

Table 8-3: The effective management of ICT resources

Parameter		λ	R^2	P-value	Significance
Factor	Indicator				
Management of ICT resources	Sufficient Networking Connection	.826	.682	***	Yes
	Database systems management	.922	.849	***	Yes
	Software and applications licensing	.881	.777	***	Yes

Furthermore, the survey also revealed that the management of ICT resources has an indirect effect (.197), through the effective planning of enterprise information security, on successful ICT risk management with both the biased-corrected p-value ($0.018-p_{bc}$) and the percentile p-value ($0.015-p_{pc}$) at a 95% confidence level. It implies that enterprise information security mediates the effective management of ICT resources to achieve successful ICT risk management. Managing ICT resources with information security control can help achieve the mitigation, avoidance and prevention of ICT risks. The adoption and implementation of the effective management of ICT resources was shown then to also be a factor in ICT risk management success in Thai business organisations.

8.1.3 The enterprise information security plan

The third factor that emerged as having an impact on ICT risk management in the Thai organisations related to the various components of the enterprise information security plan. In the analysis of the survey, consistent management and planning of people and their behaviour in an organisation, the control mechanisms of implementing organisational information security, the development of both corporate and operational plans were shown to combine to impact on ICT risk management as the factor enterprise information security.

Consistent management and planning of people and their behaviour in an organisation

The interviewees argued that the effective management of staff and their behaviour in their organisations included four areas of focus: defining the responsibility of employees, securing and protecting information security with regard to employees' behaviour in the organisation, and providing training and education programs for staff. By addressing all four areas, they believed, would ensure that operational risk related to ICT could be mitigated, risk avoided and prevented in order to achieve successful ICT risk management.

The respondents in the case studies noted that the effective management of people in the organisation affected the planning of control responsibilities of employees at both the corporate and the operational levels in ICT risk management. In the case studies, it was clear that the planning of control responsibilities of employees at the corporate level was used to balance the bottom-up control aspects developed at the operational level. Senior management at the corporate level set up committees to take responsibility for addressing all identified risks (e.g. business risks, ICT risks and IS risks). On the other hand, in addition managers at the operational level established practices for the operational team to account for specific risks (e.g. operational, technical and strategic risks). They then reported the results back to the committees in order to obtain a review and gain advice from the committees for further treatment of particular risks. The respondents in the case studies argued that the control responsibilities of employees were evident in three specific areas: business, technological and security directions and each had to be addressed to deal with operational risks. The control responsibilities of employees was previously discussed in research by AIRMIC, ALARM and IRM (2002), Straub and Welke (1998), Levine (2004), Hughes (2006), Willcocks and Griffiths (1994), and Willcocks et al. (2006). The findings of AIRMIC, ALARM and IRM (2002) were that the role of staff members (e.g. the board and all management levels) was to define how to achieve the objectives of risk management which included prevention, mitigation and avoidance of operational risks in ICT risk management. Defining clear roles and

responsibility of people in organisation, they believed, directly influenced the effective management of staff and their behaviour to achieve successful ICT risk management

The implementation of information security policy with regard to the behaviour of staff in organisations, the respondents revealed, was required to effectively manage people and their behaviour in organisations. The research of Ward (2005), Straub and Welke (1998), Hayat (2007), Smith and Eloff (2002), Calder and Watkins (2005, 2008), and ISO/IEC (2005) identified that the safety of information, related to confidentiality of organisational information, was an important concern for organisations and their risk management. They argued that securing information was used to prevent and protect organisational assets including information, information technology and systems. Securing organisational information in relation to employees' behaviour was shown in the case studies to be related to the control of the level of personnel access, or to the access rights of employees to information (e.g. specified information related to staff's job descriptions), to information technology (e.g. specified software and applications related to staff's job descriptions) and to systems (e.g. a specified module related to staff's job descriptions). Furthermore, the respondents in the case studies revealed that securing information security in employees' behaviour was mostly concerned with the control process governing employees during employment (e.g. training and educating program), at termination of employment (e.g. transferring to new position and quitting the position) and at change of employment (e.g. transferring to new position). Securing information in the organisation from employees' behaviour, they believed, directly influenced the effective management of people and their behaviour in their organisations.

The protection and security of information with regard to employees' behaviour (i.e. an insider threats) was revealed in the case studies thereby influencing the effective management of people and their behaviour in their organisations. The respondents argued that protection was best assured through employment agreements. They further explained that new staff were required to understand organisational regulations, rules and about access to confidential information prior to employment (i.e. through orientation programs as well as training and educating programs). Protecting information from inappropriate employees' behaviour was, they revealed, a control process to prevent operational risks occurring as a result of human abuse and/or error, whether or not intentional. In addition, employment agreements were used in the Thai business organisations to prevent the disclosure of sensitive organisational information. The Thai business organisations identified that they followed either/ or both the ISO/IEC 17799 standard and the COBIT framework in order to manage operational risk in achieving successful ICT risk management. The Thai business organisations considered that protecting information security when employing new staff was achieved by requiring

hiring staff to communicate to all new employees to follow the standards in use (ISO/IEC 2005; ITGI 2007).

Training and education programs were used for the effective management of employees and their behaviour in each of the case study organisations. These programs were used to raise awareness of ICT and ICT security. Interviewees in the case studies demonstrated that a training and education program was an imperative process to improve the understanding of staff about both ICT and ICT security risks. For example, organisational e-learning was introduced in one case study to inform employees in the organisation about the procedures related to staff producing organisational information in a secure way and the potential disasters, such as installed pirate software, that can result from ICT abuses and misuse of ICT.

Training and education programs were also raised with new employees to inform them of all organisational rules and regulations, and were also raised with current employees in order to prevent operational risk related to the use or misuse of ICT. These ICT abuses and instances of misuse of ICT were identified by the interviewees and included playing games online (e.g. a cause of computer viruses) and installing pirated software (e.g. direct effect on operational risk). In the Thai organisations ICT abuses and misuse of ICT were monitored and controlled by the operational manager in each department. The need for such education was also identified previously in research by Levine (2004), Hughes (2006b), Anderson and Choobined (2008), Byrd and Sankar (1995), McAdams (2004), and the ITGI (2007). In addition, the findings from Straub and Welke (1998); Hughes (2006) showed that human resources must be trained and educated in order to gain a thorough understanding of organisational vulnerability and of the resources required to secure organisational information and systems. In all of the Thai case studies, the ISO/IEC 17799 standard was the framework used to manage human resources. This standard enabled the Thai business organisations to define training and educational programs in the specific section on the employment process to ensure that 'all employees of the organisation must receive appropriate awareness training and other training, as well as regular updates and communications' (Calder and Watkins 2005, p. 135).

The implementation of the effective management of employees and their behaviour then required controlling roles and responsibilities, securing and protecting information security regarding staff's behaviour, and providing training and educating programs to prevent, avoid, and mitigate operational risk. Therefore, the effective management of people and their behaviour in this research supported the previous research (Willcocks et al 2006). Willcoks and Griffiths (1994), and Willcocks et al. (2006) which argued that the skills and abilities of human resources contribute to help the organisation boost business performance to deal with operational risks for succeeding ICT risk management. The

effective management of people and their behaviour in the case studies was seen to positively influence both the corporate level and operational plans when seeking to achieve successful ICT risk management in the Thai organisations. However, the survey analysis in this research indicated that the effective management of employees and their behaviour combined with the effective management of organisational information security thereby having structure similarity.

The control mechanisms of implementing organisational information security

The interviewees in the case studies revealed that information security was implemented to control both information and information systems. The control mechanisms of information security were used to protect and secure both data and information integrity. The respondents in the case studies revealed that the control mechanisms included the determinations of protecting and securing both data and information integrity. The determinations used were the setting of system configurations, defining access control policy, managing data and information integrity, complying with security rules and regulations, both internal and external, protecting data and privacy, and protecting the physical environment. They believed that those determinations positively influenced the effective management of organisational information security to mitigate, prevent and avoid technical or security risks in successful ICT risk management in their respective organisations.

The respondents further argued that the setting of system configurations was required to effectively manage information security and achieve successful ICT risk management.. Configuration setting was undertaken in operating systems (e.g. Windows server, Linux and UNIX), in networking operating systems (e.g. Netware and Cisco), in business software (e.g. SAP and business solution software) and in hardware systems and operations (A/S 400, Hubs, Switches and Routers). The case study interviewees believed that information security operations that caused technical risk were prevented, avoided and mitigated because a malfunction of ICT or systems could not occur. The organisations studied adopted both the ISO/IEC 17799 standard and the COBIT framework to deal with the issue because they provided frameworks, either at the senior management or operational levels, to enable them to institute processes for managing technical or security risk associated with the use of ICT (ISO/IEC 2005; ITGI 2007).

The respondents in the case studies revealed that another control mechanism of the effective management of organisational information security was development and implementation of an access control policy. This supported the findings in previous research from Calder and Watkins (2005) and Milenkovic (2008) who claimed that access control must be defined for all business participants (e.g. users, administrators, ICT persons and internal auditors). In the case studies, access control policy was focused on

the level of access rights to network systems and personal computers. Each of the organisations revealed that the need for official documentation of access control policy was required to maintain and review access control rights on a regular basis. The official document of access control policy in the Thai organisations included defining only authorised persons to have access to network services, using both user allocation and password management systems to limit the level of access to computers and systems and monitoring access of log files to prevent unauthorised access. In the Thai case studies, logical access controls were used to protect and secure sensitive organisational assets such as raw data, information, information technology and systems. Again the case studies adopted both the ISO/IEC 17799 standard and the COBIT framework to enable the effectiveness of access control policy (ISO/IEC 2005; ITGI 2007).

The respondents in the case studies revealed that management of data and information integrity was important because these organisations were using information security to monitor and secure the processes of producing data (i.e. input process), storing data (i.e. processing process) and disseminating information (i.e. output process) throughout the organisation and with stakeholders. Smith and Eloff (2002); Hawkins et al. (2003); Hayat et al. (2007); Flowerday and Solms (2005); ISO/IEC (2005); ITGI (2007) had previously shown in their research that maintaining data and information integrity were important in the organisation when dealing with technical or security risks. The respondents in the Thai organisations noted that validation check applications were used to maintain data and information integrity. Validation check applications were used to validate data appropriateness before putting data into applications and systems, to detect any corruption of information through processing errors and deliberate acts and to validate output data from applications systems for its correctness and appropriateness before being distributed. These processes were controlled and monitored in the Thai organisations to ensure that their data and information had integrity. For example, one organisation adopted penetration tests and security scanning tools to monitor and control all organisational transactions in order to ensure that all business transactions were performed properly and correctly.

Data protection and privacy were another element of the effective management of organisational information security. Anderson and Choobineh (2008), and Księżopolski and Kotulski (2007) had previously shown in their research that protection of information assets on every staff level in organisations must be secured. Data protection and privacy for the Thai organisations related to the protection from both external and internal threats to personal privacy such as malware, viruses, and worms from staff email and personal files (e.g. songs, movies and animated pictures) brought in from outside the organisation. The internal threats problem, they noted, could be controlled, by using software-scanning tools that automatically detected threats posed by staff misuse. For

example, pirated software installed on personal computers in the organisation could be detected, after which software scanning tools would automatically remove unwanted software from the computers in order to prevent, protect against and avoid any harm related to technical or security risks. Only one of the Thai organisations took action to include this in their ICT risk management processes.

Security compliance was another critical element in the effective management of information security that emerged from the case studies, in part as a result of the Royal Thai Government having enacted the *Computer Crime Act* regarding computer abuse (AHRC 2007). McEvoy and Whitcombe (2002) had argued that security compliance entailed clarifying the details of organisational information security. Organisational information security covered prevention, mitigation and avoidance of threats, and vulnerability of organisational assets including internal and external impacts. Moreover, organisational rules and regulations were also involved because the respondents in the case studies argued that their organisations needed to ensure that all ICT and ICT security procedures and processes were performed appropriately and correctly. The respondents revealed that ensuring security compliance was elaborated in their ICT risk management process and to do this they adopted the ISO/IEC 17799 standard (ISO/IEC 2005) and part of the COBIT framework (ITGI 2007).

The setting of system configuration, managing and documenting access control policy, managing data and information integrity, protecting both data and privacy and regularly reviewing and updating security compliance were required to effectively manage organisational information security. The effective management of organisational information security was seen to positively influence the planning at the corporate and at the operational levels when seeking to establish successful ICT risk management in the Thai organisations interviewed.

In the survey analysis in this research, the statistical results suggested that merger of the effective management of employees, and of organisational information security reflected that the effective management of information security was required to secure and protect information security regarding employees and their behaviour, information, applications and systems (Table 8-4).

Table 8-4: The first merger

The effective management of employees (HRMP)				Organisational information security (OS)				ρ^2	Implication
	R^2	ε	AVE		R^2	ε	AVE		
sum	2.846	1.684	0.628	sum	3.406	0.744	0.821	0.762	The AVE value of HRMP is not greater than the squared correlation between both factors (ρ^2). As a result, the merger of both factors was undertaken in discriminant validity test.

Based on this combination, the effective management of organisational information security was proposed as a new construct in the model analysis. The statistical results showed that the correlation between both key factors was .87 in the discriminant validity test; as a result, it indicated structure similarity (Chapter 7, p. 205). The combination supported the recommendations of the ISO/IEC 17799 standard because managing people and their behaviour in an organisation and managing information security were included and recommended in its standard as information security management (ISO/IEC 2005).

The corporate plan

ICT risk management was always planned at the corporate level in the Thai organisations. A corporate plan represented the procedures used for ICT risk management as the overall plan for the organisation. This research did not, however, focus on the degree of control used (i.e. strategic level, operational level and tactical level) (Segar & Grover 1996; Shortreed et al. 2000; Anderson & Choobined 2008), but rather on the level of management, because these approaches (i.e. the top-down approach and the bottom-up approach) can help the organisation strengthen the effectiveness and efficiency of its plan at both the corporate level and the operational level (Earl 1989; Bandyopadhyay et al. 1999; Schultz 2007). To strengthen a plan at the corporate level, the respondents in the case studies argued that ICT risk management planning was needed and then used to set the process of treatment of ICT risk problems as the scope of ICT risk management which would then drive the operational plan. The value of the corporate level plan was also supported by Martin (2003, p. 3) who described how an organisation 'adopted a management perspective that seeks to identify the integrated set of broad factors, both strategic and operational, that influence the current practice of configuring the architecture, resources and methodology elements in organisational ICT risk management.' The respondents in the Thai organisations revealed that the effectiveness of a corporate plan included defining the details of ICT processes, the details of ICT control and audit plan and classification of information technology for dealing with ICT risk management successfully.

ICT control and audit plans were also identified as important in the case studies as helping the organisation to provide the guidelines for ICT control, particularly in regard to ICT processes included in a corporate plan. ICT control and audit plan was seen by the respondents to directly influence the effectiveness of a corporate plan to achieve successful ICT risk management. ICT control and audit covered technological functions that fitted organisational policies. A corporate plan was also considered in the COBIT framework, which explicitly showed that the aim of ICT control at the corporate level in an organisation is to achieve effective ICT management of the risk in business processes (ITGI 2007). In addition, assessing and managing ICT risks in the COBIT framework were

the preliminary focus to plan a brief overview of ICT applications control and ICT security control. Solms (2005a) suggested that the COBIT framework also helped the organisation develop guidelines for ICT risk management at the senior management level by providing a framework for control processes.

Classification of ICT in ICT risk management was also considered as important by the respondents in the case studies because ICT applications and ICT security were distinct from each other. This determination was seen in the Thai organisations to directly affect the effectiveness of a corporate plan when dealing with successful ICT risk management. This classification of ICT was mainly a focus when considering how to deal with ICT risk. Classification of ICT helped the Thai organisations distinguish between the degree of control of ICT itself and control of ICT security. Therefore, identifying the scope of ICT applications and ICT security needs, at the corporate level through a corporate plan, provided an overview of the appropriate treatment of ICT and ICT security in the organisation. This classification of ICT is also a key element in both the COBIT framework and the ISO/IEC 17799 standard (ITGI 2007; ISO/IEC 2005), adopted by the organisations studied. According to ITGT (2007), the COBIT framework explicitly shows the difference between application controls and ICT general controls in order to simplify their difference to the organisation As a result of their adoption by the Thai organisations, general controls were embedded in their ICT processes and services including systems development, change management, security and computer operations (ITGI 2007). Application control also was embedded in business process applications to ensure completeness, accuracy, validity, authorisation and segregation of duties defined as data and information integrity (ITGI 2007). Moreover, ICT control processes within the COBIT framework are defined by a complete set of high-level requirements at the executive level and these too were clearly adopted in the Thai organisations studied.

The effectiveness of the corporate plan was essential, the respondents in the case studies believed, and that the senior management directly influenced the planning of ICT risk management in the Thai business organisations. In providing an ICT risk management plan, the survey analysis showed that a corporate plan positively affected an operational planning at the operational level when seeking to achieve successful ICT risk management.

The operational plan

The respondents Thai organisations studied argued that operational managers also planned for successful ICT risk management at the operational level. They further elaborated that an operational plan was used to define the procedures and methodology to deal with ICT risk at all of the operational levels. An operational plan outlined the details of ICT risk management for each of the departments in Thai business

organisations. Moreover, an operational plan was produced based on the corporate plan to expand the details of the realisation of a corporate plan throughout the organisation. The respondents revealed that the effectiveness of an operational plan derived from a number of actions including defining and implementing information security control and audit processes, defining a clear outline of technical security measures and managing ICT project risks in each department. These determinations, the interview data showed, positively affected the success of ICT risk management planning in the corporate plan.

Defining and implementing information security control and audit processes regarding ICT risk management was the key element of the operational plans in the Thai organisations. It was important to align with organisational policy and plan with the corporate plan and the principles in the two standards use in order to outline the procedures of the ICT risk management methodology in detail for each department in the Thai business organisations, confirming the research conclusions of (Haworth & Pietron 2006) and Solms (2005a)

Defining clear details of technical security measures in an operational plan was the other element that the respondents in the Thai case studies revealed in relation to establishing a plan for dealing with ICT risks at the operational level. The details of technical security required clarity to determine appropriate technical controls in each department. The outline of technical security measures emerged in each organisation from the ISO/IEC 17799 standard, which stated that the details of control objectives in particular functions were required to be followed and adapted in the organisation (ISO/IEC 2005). In this regard, risk analysis and management in the ISO/IEC 17799 standard were the focus to plan the details of technical security in the Thai organisations studied.

Lastly, managing ICT projects was also highlighted as an important element of an operational plan, in so far as software development treated ICT risk management on a project-by-project basis. Therefore, managing ICT project risk was also considered in this research in terms of raising awareness in the organisation of ICT infrastructure changes or ICT project changes. The focus on ICT project risk management was to provide a methodology for dealing with ICT projects in order to manage ICT risks as they occurred in each new project. The important of managing ICT projects well was noted by Martin (2003, p. 6), who stated that 'ICT risk management is not only a prerequisite for successful project configuration, but it is a marketable competency'. Martin (2003) further argued that the methodology of ICT project risk management was not only used to manage an ICT project itself but also to manage operational and strategic risk embedded within the ICT project. The adoption of these processes in the Thai organisations confirmed this.

In the analysis of the survey data the initially separate factors, a corporate plan and an operational plan, were merged to a single factor, 'The Enterprise Level Plan' (Chapter 7, p. 210). The main justification for the combination was that Thai business organisations believe that managing organisational information security was considered at both the corporate and the operational levels and that this was a key element in ICT risk management success (Table 8-5).

Table 8-5: The second merger

The corporate level plan (CLP)				The operational level plan (OLP)				ρ^2	Implication
	R^2	ε	AVE		R^2	ε	AVE		
sum	3.047	1.452	0.677	sum	3.039	1.726	0.638	0.808	The AVE values of both factors are not greater than the squared correlation between both factors (ρ^2). As a result, the merger of both factors was undertaken in discriminant validity test.

This conclusion supported previous research by Weill and Ross (2004) and Brown and Nasuti (2005) and Caralli (2004, p. 14), who argued that managing enterprise information security 'is intended to impart the need for active planning, controlling and coordination of activities across an enterprise so that security goals can be reached'.

The effective management of staff and their behaviour, the effective management of organisational information security, and the effective planning of both the corporate and the operational levels, were shown in this research (Chapter 7, p. 214), both in the interviews and as a result of analysis of survey data of Thai organisations to be best viewed as a single success factor, 'Enterprise Information Security Plan' (Table 8-6). The effective planning of enterprise information security was shown to be required at both the corporate and the operational levels to set the organisations' ICT risk management plan for information security at an enterprise-wide level.

Table 8-6: The third merger

Organisational security management (OSM)				The enterprise level plan (ELP)				ρ^2	Implication
	R^2	ε	AVE		R^2	ε	AVE		
sum	3.373	0.777	0.813	sum	3.332	1.039	0.762	0.781	The AVE value of the enterprise level plan is not greater than the squared correlation between both factors (ρ^2). As a result, the merger of both factors was undertaken in discriminant validity test.

At this enterprise level, the research demonstrated that defining access control policy, managing data and information integrity, complying with security rules and regulation and protecting data and privacy were a number of key elements affected success (Table 8-7).

Table 8-7: The effective planning of enterprise information security

Parameter		λ	R^2	P-value	Significance
Factor	Indicator				
Enterprise information security plan	Access control policy	.900	.810	***	Yes
	Data and information integrity management	.950	.903	***	Yes
	Security compliance	.932	.869	***	Yes
	Data protection and privacy	.890	.792	***	Yes

Defining access control policy was the first key element in the effective planning of enterprise information security by the Thai business organisations. Access control policy defined the protective process that monitors and controls physical and logical organisational assets. Physical access control was previously highlighted as important in the study of Badenhorst and Eloff (1994), who mentioned that physical access security must be monitored to prevent theft of an organisation's information, information resources and assets. In addition, logical access control was supported by the research of Hayat et al. (2007) and Milenkovic (2008) who revealed that logical access controls were needed to secure ICT infrastructure.

Managing data and information integrity was the second critical element in the effective planning of enterprise security. Thai organisations believed that managing data and information integrity involved monitoring control processes with regards to preventive, and corrective processes within input, processing and output (IPO) confirming what had been shown elsewhere (Moeller 2005). Managing data and information integrity in the Thai organisations focused on protecting data by a secure means during the input (raw data) through the processing (correcting, storing and preventing information) through to disseminating the information to the stakeholders. The importance of this element of managing data and information integrity supported conclusions in previous studies by Bojanc and Jerman-Blažič (2008), Flowerday and Solms (2005), Coles and Moulton (2003), and Smith and Eloff (2002) who all argued that confidentiality, integrity and availability (CIA) of organisational information assets must be maintained. In addition, in terms of managing data and information integrity, the COBIT framework, used in the Thai organisations, covered the control process of information integrity focusing on completeness, accuracy and validity (Boritz 2005). Conversely, managing data and information integrity was more thoroughly considered in and supported by the ISO/IEC 17799 standard, which thus supplemented timeliness, authorisation and security omitted in the COBIT framework (ISO/IEC 2005). Since the majority of Thai organisations used

both standards, all areas of need for risk management in the enterprise plan were covered.

Complying with security rules and regulations in Thai organisations was another key element in the effective planning of enterprise security. The reason given was that all security rules and regulations both internal and external to the organisation were needed to be considered when dealing with ICT risk management. Complying with organisational security rules and regulations was required in the Thai organisations to regularly check ICT facilities to ensure maintenance of security implementation standards and to regularly review the effective planning of enterprise security to ensure compliance with organisational security policy and standards. Complying with security rules and regulations in the organisation and external regulators were shown to be significant and to be supported by the adoption of the ISO/IEC 17799 standard which elaborated the details of security compliance (ISO/IEC 2005). In addition, national regulations and laws generated by external regulators such as the Stock Exchange of Thailand (SET), the Security Exchange of Thailand (SEC), the Bank of Thailand (BOT) and the Royal Thai Government were also considered in each organisation in order to help the Thai business organisations prevent and avoid the operational, strategic and technical risks related to ICT risk management.

Protecting data and privacy was the last element identified in this research critical to the effective planning of enterprise security when dealing with ICT risk management successfully in Thai business organisations. Data protection and privacy involved the monitoring process that maintained data protection and privacy in the Thai business organisations. The significance of protecting data and privacy for the Thai organisations corresponds with similar conclusions in research by Hughes (2006b); Hilton (2009); Kenny (2004) and Martínez et al. (2010), who each suggested that data protection and privacy must be implemented in order to facilitate advances in risk management technology.

This research then proposes that the effective planning of enterprise information security is a key success factor for planning ICT risk management in Thai business organisations. The statistical results in this research indicated that the effective planning of enterprise information security was important in dealing with ICT risk management. This research showed that relationships between enterprise security plan and successful ICT risk management were significant with both the biased-corrected p-value (0.026−pbc) and the percentile p-value (0.024−ppc) in a 95% confidence level (Chapter 7, p. 233). Enterprise information security planning together with organisational policy and the management of IT resources emerged as the three key factors in Thai organisations efforts to achieve successful ICT risk management.

8.2 Key factors in successful ICT risk management

In summary, the extant literature, and both of the standards uses in ICT risk management from a governance perspective, have highlighted separate and sometime overlapping factors that have a significant influence on organisations being successful with ICT risk management. These are summarised in Table 8-8.

Table 8-8: A summary of key factors of successful ICT risk management in previous research, in the COBIT framework and in the ISO/IEC 17799 standard (Repeated from Table 2-7)

Research Literature	The COBIT framework (focused on at the highest appropriate organisational level)	The ISO/IEC 17799 standard (focused on at the operational level)
Relevant policy in place (Benaroch et al 2006; Buckby et al. 2009; Capuder 2004; Cha et al. 2008; Colbert & Bowen 1996; Fletcher 2006; Gallegos et al. 2004; Khan 2006; MyEvoy & Whitcombe 2002; Segars & Grover 1996; Smith & McKeen 2006; Solms 2005a)	Creating ICT policy to define a strategic ICT plan and to determine technological direction	Creating information security policy to document information security policy and to review of the information security policy.
Policy and mechanisms in place to protect ICT resources such as information assets, ICT infrastructures and ICT architecture (Benaroach et al 2006; Bodnar 2006; Buckby et al. 2009; Byrd et al. 1995; Fletcher 2006; Longstaff et al. 2000; Smith & Eloff 2002; Stoneburner et al. 2002; Straub & Welke 1998)	Effective ICT resource management with regard to ICT infrastructure, ICT performance, ICT project,	Not clearly defined
Policy and mechanisms in place to manage human resources and defining roles and responsibilities (Badenhorst & Eloff 1994; Ciborra 2006; Figg 1999; Hughes 2006a; Moulton 2003; Van Grembergen & De Haes 2008; Willcocks & Griffiths 1994; Willcocks et al. 2006)	Constant management of human resource including training and educating programs.	Constant human resource security for employees during employment and termination or change of employment
Policy and mechanisms in place to manage access control in physical and logical systems (Badenhorst & Eloff 1994; Hayat et al 2007; Levine 2004; Milenkovic 2008; Schultz 2007)	Creating a process for managing the physical environment	Creating a process for secure areas, equipment security, user access management, user responsibilities, network access control, operating system access control and application and information access control.
Policy and mechanisms in place to manage business continuity planning	Creating a continuous services plan	Creating business continuity management and information security incident planning and

(Cha et al. 2008; Groves 2003; ISO/IEC 2005; ITGI 2007; Posthumusa & Solms 2005)		management
Implementation of control mechanisms to secure information, information systems and assets (Bodnar 2006; Byrd et al. 1995; Karabacak & Sogukpinar 2006; Lainhart 2001a; Longstaff et al. 2000; Smith & Eloff 2002; Stoneburner et al 2002)	Implementation of an ICT plan (e.g. defining ICT processes) regarding the ICT infrastructure and for developing of a security culture	Implementation of the organisation of information security and asset management to create an ICT security plan (e.g. defining information security processes)
Implementation of control mechanisms to protect information integrity such as input, processing and output (IPO) processes (Bojanc & Jerman-Blazic 2008; Coles & Moulton 2003; Flowerday & Solms 2005; Hermanson et al 2000; Moeller 2005; Saint-Germain 2005; Smith & Eloff 2002; Theoharidou et al. 2005)	Implementation of ICT processes, technology infrastructure, and data management	Implementation of information systems development and maintenance
Implementation of control mechanisms to protect threats and vulnerabilities of assets (Anderson & Choobineh 2008; Hawkins et al. 2003; Karabacak & Sogukpinar 2006; Ksiezopoliski & Kotulski 2007; Smith & Eloff 2002)	Not clearly defined	Implementation of organisation of information security; internal organisation focusing on vulnerability of assets and external environment focusing on threats.
Operationalisation of ICT management control (Elieson 2006; Eloff & Eloff 2003; Finne 2000; Flowerday & Solms 2005; Gerke & Ridley 2006; Khan 2006; Liu & Ridley 2005; Ridley et al. 2004; Robinson 2005; Smith & Eloff 2002; Smith & McKeen 2006; Van Grembergent et al. 2004)	Implementation of ICT processes to control ICT management	Not clearly defined
Operationalisation of information security control (Capuder 2004; Eloff & Eloff 2003; Fletcher 2006; Flowerday & Solms 2005; Hayat et al. 2007; Kenning 2001; Khan 2006; Robinson 2005; Smith & McKeen 2006; Solms & Solms 2005, 2006; Solms 2005a; Straub et al. 2008)	Not clearly defined	Implementation of information security processes to control information security management

In the extant research literature there are a number of themes that emerge as factors impacting on successful ICT risk management in organisations. Ciborra (2006) argued that risk management emerged from people in an organisation having a lack of knowledge, from the role of biased data when assessing risk in organisations and from the influence of internal politics. Levine (2004) and Hughes (2006a) added that a lack of clarity of the roles and responsibilities of people impacted on successful risk management. Straub et al (1998) argued that human resource management is considered significant whilst dealing with ICT risk management. The reason is that the organisation needs senior management support in order to gain a thorough understanding of organisational vulnerability and of the resources required in securing organisational systems. It is necessary that senior management understand the security actions required and for them to integrate security planning into information security policy through adoption of organisational standards, and that users are trained and educated about security awareness in order that organisational standards can be reviewed and updated. Staff at all levels can help reduce operational and technical risks; therefore, training programs, clarification of roles and responsibilities, and the identification of specific authority for specific roles must be provided for all staff (Hughes 2006a) to ensure success risk management.

Smith and Eloff (2002) argued for a different emphasis, that ICT risk management was defined in terms of information and communication technology (ICT) and information security (IS) components. Specifically the ICT component is used to describe the scope of the ICT domain where ICT produces data throughout input, processing and output (IPO) and disseminates information to internal and external parties (Smith & Eloff 2002). This is used to control the ability of ICT used in IPO processes particularly in relation to ICT risks. Byrd et al. (1995) further suggested that effective ICT related architecture helped an organisation define the strategy to drive, shape and control its architecture when dealing with ICT risk management. ICT architectures are specified by what types of hardware and software are employed; where personnel, equipment, data and facilities are located; the levels of applications, data and procedural compatibility that exist across locations (e.g. department to department, business unit to business unit); and how locations are connected, coordinated, and controlled (e.g. telecommunications networking) (Byrd et al. 1995).

Smith and Eloff (2002) also argued that another component of ICT risk management was information security (IS). Schultz (2007) provided guidance on how to mitigate ICT risks with regard to information security through proper management of physical security systems such as devices, process control systems and ICT infrastructure. Schultz (2007) further explained that for successful ICT risk management in organisations that senior management are responsible for understanding the configuration of networks, systems

and ICT infrastructure, use of penetration tests, for supporting to management and audit functions, and for developing organisational information security policies (e.g. a corporate plan and an operational plan−a technical means). However, 'many senior managers are unaware that ICT security in their organizations is inadequate what the consequences of vulnerability may be' (Byrd et al. 1995, p41). Information security is used to describe the security domain where data and information is protected and rendered with 'identification and authentication, authorization, confidentiality, integrity and non-repudiation' (Smith & Eloff 2002, p. 268).

This research built of those previously identified factors with reference to the most commonly accepted and used standards. From a different perspective the two standards addressing governance of ICT in business organisations focus on other factors as being more influential on successful ICT risk management. The COBIT framework is recognised as a top-down or high-level framework for governance and control over ICT risk (Khan 2006; Smith & McKeen 2006). The main purpose of the COBIT framework is to clarify business-focused, process-oriented, control-based and measurement-driven objectives and requirements through business process and ICT systems in an organisation (ITGI 2007). The COBIT framework was established as ICT control practices to help senior management direct their responsibility with regard to an organisation's assets by aligning the requirements in terms of business risk, control needs, and technical issues (Bodnar 2006). The COBIT framework also describes the information process requirements that match the broader classes of ICT control used by an organisation to achieve its objectives and goals (Bae et al. 2003).

The COBIT framework assists senior management to build ICT processes and controls which are appropriate for implementing and developing ICT governance and management for dealing with strategic and operational risks in ICT risk management (Smith & McKeen 2006). The COBIT framework provides senior management with management strategies for ICT resources in four domains: planning and organising; acquiring and implementing; delivery of services and support; and monitoring and evaluating (ITGI 2007). Within these four domains, the framework defines how ICT infrastructure and systems can be managed and controlled to support ICT functions for users and how ICT infrastructure and systems can be maintained to ensure that ICT performance meets business objectives and goals (ITGI 2007). As a result, the COBIT framework emphasises the policy for and management of ICT infrastructure and systems when dealing with ICT risk management (ITGI 2007). Policy is considered in the COBIT framework to provide the clear direction of the role and responsibility of executives and the Board of Directors to manage ICT related risks (ITGI 2007). In addition, management of ICT risk management is considered in the COBIT framework to assure that ICT

processes and controls can maintain the value of ICT, and ensure that the enterprise's ICT supports business objectives.

The ISO/IEC 17799 standard provides a focus on the details of organisational information security practices (ISO/IEC 2005). This standard is used more as a set of lower-level guideline that details the specifics of how information security must be done for dealing with strategic, operational and technical risks in ICT risk management (Solms 2005a). Furthermore, this standard is the focus of information security control at the operational level and helps the operational manager define precisely how control objectives can be used to achieve business objectives and goals in terms of their technical directions (Solms 2005a).

The ISO/IEC 17799 standard helps an organisation manage information security in defining asset management, physical security mechanisms and access control; in documenting information security policy and operational procedures; in reporting security incidents and in business continuity management (Myler & Broadbent 2006). Information systems security refers to the protection of all information system elements and the safeguarding of information integrity; that is, confidentiality, integrity and availability (Theoharidou et al 2005).

The ISO/IEC 17799 standard helps the operational manager assign information security roles and responsibilities (Groves 2003). By doing so, staff at different levels are responsible for different perspectives of the standard. For example, senior management is concerned with creating information security guidelines, the organisation of information security, human resource security, business continuity management and for compliance. Furthermore, at the operational level managers are concerned with taking action on technical matters such as setting access control policy, data and information integrity management, data protection and for dealing with privacy. Theoharidou et al. (2005) mentioned that implementing the ISO/IEC 17799 standard can help an organisation deal with insider threats by providing the control objectives regarding job descriptions of security staff, personnel screening, confidentiality agreements, security responsibility in the terms and condition of employment, and information security and training. Therefore, the ISO/IEC 17799 standard mainly focuses on technical or security policy, information security management and human resource management as supporting successful ICT risk management. Technical or security policy is considered to supplement the setting of ICT policy for the executives and the Board of Directors in the organisation to deal with ICT risk management. Human resource management is considered important in the ISO/IEC 17799 standard to provide information security during employment and for associated ICT risk management.

8.3 Successful model for ICT risk management

The sets of factors (creating policy, management of ICT resources, management of information security, constant management of human resource issues, implementation of a corporate plan and an operational plan) were tested in this research initially in a number of business cases in Thailand. From the analysis of the case studies, a set of factors were identified; that affect successful ICT risk management:

- creating ICT policy (e.g. defining a strategic ICT plan and determining technological direction), Information security policy (e.g. documenting a brief of information security policy and reviewing information security policy) and a continuous service plan (e.g. planning and managing business continuity management and information security incident),

- effective management of ICT resources (e.g. a process for managing ICT infrastructure, ICT performance and ICT project,

- effective management of information security (e.g. a process for securing and managing the physical environment and logical systems such as equipment security, user access management, user responsibilities, network access control, operating network access control, operating system access control and application, and information access control),

- constant management of human resource issues (e.g. training and educating programs and defining roles and responsibilities), and

- implementing both a corporate plan and an operational plan (e.g. controlling ICT processes for maintaining information integrity and controlling IS processes for securing information, information systems and assets

These factors were then used together with the principles in the COBIT framework and the ISO/IEC 17799 standard to define relationships in the development of successful ICT risk management (SICTRM). These factors were:

- effective creation of organisational policy (POLICY),

- effective management of ICT resources (IT),

- effective management of information security (OS),

- effective management of people and their behaviour (HRMP),

- effective planning of ICT risk management at both the corporate level (CLP) and at the operational (OLP) level.

These were then built into a model of success in ICT risk management (Figure 8-1)

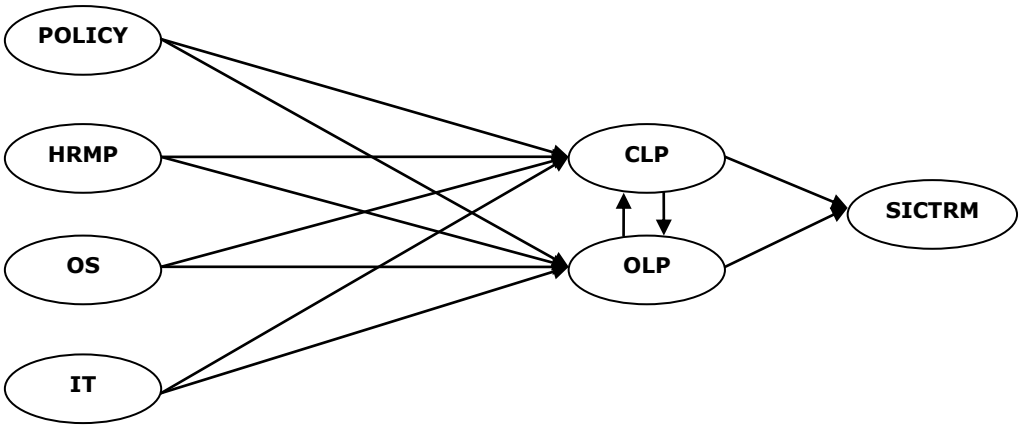


Figure 8-1: A conceptual model for successful ICT risk management (Repeated from Figure 6-1)

The model was then tested as a whole to determine the strength of the relationships hypothesised in the model to impact on successful ICT management. The outcomes of the survey analysis showed that the following factors were more influential:

- implementation of organisational policy,
- effective management of ICT resources and
- planning of enterprise security.

A discussion of the findings from both the case studies and the survey of this research were compared those findings with previous research and to draw implications for what the research has added to what we already know.

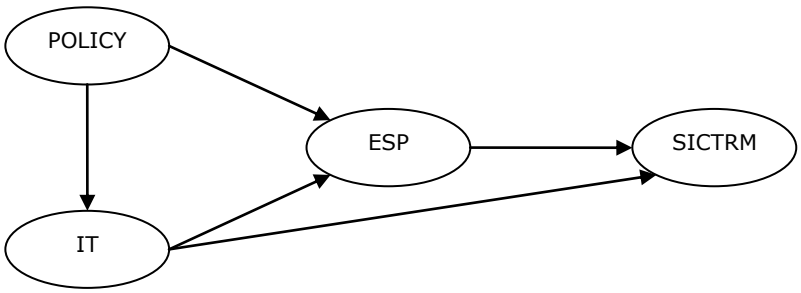


Figure 8-2: A successful ICT risk management model

The objectives of this study were to understand the key factors that are indicative of success in ICT Risk Management in Thai businesses. Results from both the case studies and the survey analysis indicated that effectively creating organisational policy, managing reliable ICT resources and planning enterprise information security were clear success factors for ICT risk management when dealing with operational, technical and

strategic risks related to ICT (Figure 8-2). Therefore, this research proposed new relationships among the success factors in the model. In the model, creating organisational policy directly affected managing ICT resources and planning enterprise information security that succeeded ICT risk management. In addition, the effective management of ICT resources directly affected both the effective planning of enterprise information security and successful ICT risk management. Lastly, the effective planning of enterprise information security was shown to directly affect successful ICT risk management.

8.4 Summary and Contribution

The research outcomes have confirmed the suggestion of Solms (2005a) that information security must be considered at both the corporate level (e.g. by senior management) and at the operational level (e.g. by the operations manager) through the development of clear policy. The effective creation of organisational policy was the focus of Thai organisations to force all staff to recognise awareness of business direction when dealing with ICT risk management. ICT policy and Information security policy were required in the Thai organisations to plan ICT and IS use and to support that use with effective risk management processes. A policy document of organisational policy for ICT risk management was created in the Thai organisations to cover documenting risk, the roles and responsibilities for risk management, risk management methodology, risk control and auditable areas.

Firstly, roles and responsibilities for risk management was the focus on the control of people and their behaviour in organisations. This control was considered as one of risk management component that was the determination of the organisation when dealing with ICT risks. Roles and responsibilities were defined at the Board of Director by separating the committee to take responsible for different actions in dealing with ICT risks to achieve the organisation's objectives and goals. They were also defined at the operational staff to be accountable for their own task to cooperate with the senior management level in achieving organisation's objectives and goals for dealing with ICT risks. Secondly, risk management methodology was also defined by both the senior management and the operational level in order to put risk under control. ICT processes, IS processes and ICT projects were elaborated the details of their own actions in the control and audit plans. The planning of the control and audit processes was separately determined each auditable area by both the senior management and the operational managers as a consensus enterprise plan. Lastly, risk management control was the focus on technology and facilities, and information security in both people and their behaviour and systems in organisations. This risk management control was required to secure the

both ICT and IS processes in order to maintain data and information integrity. The effectiveness of ICT and IS processes ensured that sensitive and confidential information in organisations was undertaken through IPO processes in a secure manner.

This research has identified and then confirmed a number of key elements affect ICT risk management success in Thai organisations. These are shown in Figure 8-3. This model proposes that for successful ICT risk management an organisation should begin with the planning of ICT risk management. Senior management need to consider policy development as the first phase of planning. This clarifies ICT use objectives, IS objectives and assists in development of a document of organisational policy (e.g. risk statements) as elements of the overall plan. The effective management of ICT resources is then necessary to follow in order to achieve an ICT risk management plan for an organisation. The planning of enterprise information security is also necessary to obtain support from both senior management and operational managers to build up consensus agreement on information security. Based on the research findings, an organisation can succeed in its ICT risk management planning through realisation of each of these operational and strategic areas. As a result, it can be argued, this model can be used as a successful ICT risk management framework for dealing with operational, technical and strategic risks related to ICT in an organisation.

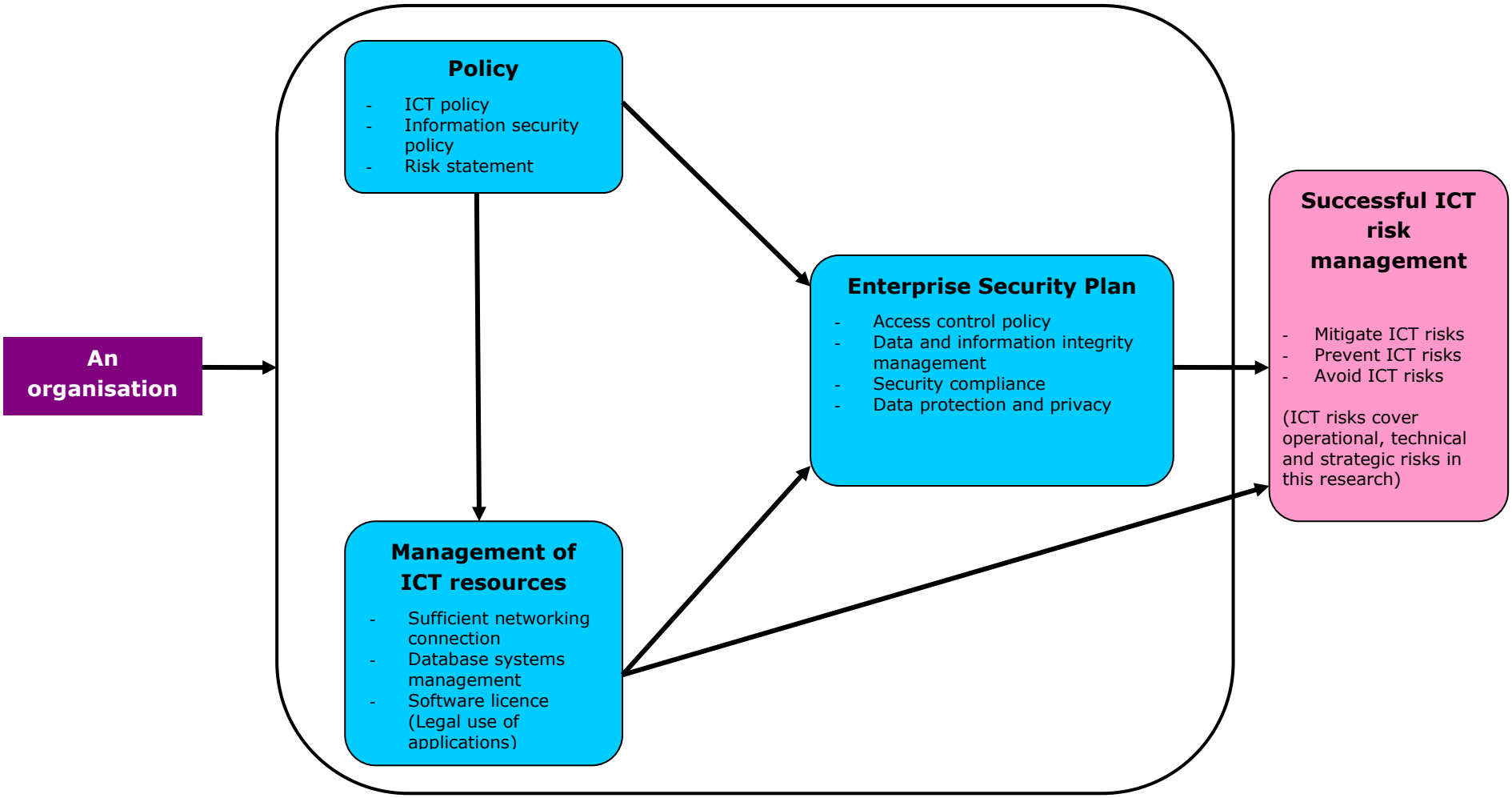


Figure 8-3: A success model for ICT Risk Management in Thai business

The first major contribution of this research was to suggest to the practitioner that an organisation is required to define its own policy and objectives to achieve successful ICT risk management. Although, the research recommendation of defining ICT risk policy is not new, it extends the understanding of substantial previous research and illustrates the advantages of managing risk through the adoption of governance standards such as the COBIT framework and the ISO/IEC 17799 standard. This research has also extended that understanding by showing that effective and successful ICT risk management must work at both the strategic and operation management levels in an organisation. There is a clear role and responsibility for ICT risk management at both the senior management and the operational staff levels to be required to define action for preventing, avoiding and mitigating strategic risk related to ICT. This research also extends this understanding of ICT risk management embedded in the governance standards in showing that planning at an enterprise-wide level, and integrating human resources management and managing of ICT resources together have a clear impact on the outcomes of ICT risk management.

The second major contribution of this research was to provide evidence of the value of the integration approach of using both the COBIT framework and the ISO/IEC 17799 standard. This research has shown that ICT governance (i.e. the COBIT framework) and IS governance (i.e. the ISO/IEC 17799 standard) can be integrated as one single management framework for dealing with ICT risk management. The integration of the COBIT framework and the ISO/IEC 17799 standard as the two-way approach to ICT risk management works well. While the COBIT framework lays the foundation of the top-down approach to risk management; the ISO/IEC 17799 standard supports bottom-up risk management. By doing so, this research firstly compared the profile of ICT risk management practice of Thai business organisations with the control objectives in the COBIT framework and the ISO/IEC 17799 standard. The results of the case studies showed that using either the COBIT framework or the ISO/IEC 17799 standard alone did not entirely cover the practice of ICT risk management in Thai organisations. Furthermore, the results of the survey analysis confirmed that the corporate level plan and the operational level plan were combined due to having structure similarity. As a result, the COBIT framework as top-down process can be used to state the corporate plan for ICT risk management to the operational manager. The operational managers then develop the operational plan for ICT risk management to confirm the strategic plan developing them together as a consensus enterprise plan. An enterprise plan is supported by organisation theory in that neither centralisation nor decentralisation can help achieve successful ICT risk management. In contrast, both centralisation and decentralisation together can assist in achieving successful ICT risk management.

The third contribution of this research has also shown that the development and implementation of organisational policy, the effective management of ICT resources and the planning of enterprise information security together emerged as success factors to help achieve successful ICT risk management in an organisation. This research proposes that effective ICT security and ICT use policies are required for successful ICT risk management and that the control processes of the COBIT framework and the ISO/IEC 17799 standard can be used to facilitate an organisation creating their own policy. The research also showed that the control processes of the COBIT framework can be used to facilitate organisations to manage ICT resources appropriately. Lastly, the research has also shown that both the control processes of the COBIT framework and the ISO/IEC 17799 standard can be used together to facilitate organisational planning of enterprise information security. These three success factors contribute to the existing literature in terms of providing a broader understanding of what is specifically involved in successful ICT risk management planning. However there are limitations to these conclusions. The next section discusses limitations of this research.

8.5 Limitations of the research

According to 53% of unexplained variance reported in Chapter 7, p. 235, unexplained variances might result from the types of sample adopted in the qualitative and quantitative methods. The types of sample in the qualitative method include the banking and software development sectors, which may affect the validation in the quantitative method. For example, both the banking and software development sectors might consider service management as other success factors, related to other standards (i.e. the ITIL framework, the Basel II accord, and the ISO/IEC 38500:2008), when dealing with ICT risk management (ITGI 2007; Basel 2005; ISO/IEC 2008). As a result, limitations of the research are:

First, according to the recommendations of the IT governance institute (ITGI, 2005a), the information technology infrastructure library (ITIL) should be applied together with the COBIT framework and the ISO/IEC 17799 standard when dealing with ICT risks. ITIL is considered best practice for ICT service management and it helps organisations to handle ICT risks relating external threat and ICT service management. However, this research focused on the internal organisational setting rather than the external environment (i.e. third party) which is addressed by ITIL.

Second, with regard to risk management in banking institutions, adherence to the Basel II accord is compulsory for banks around the world. Although, banking institutions in Thailand were studied in this research, the Basel II accord was not discussed because it was out of the scope of this research. The researcher therefore notes that in future the

Basel II accord should be considered and included in the process of data collection in order to enhance understanding of whether banks focus on the Basel II accord alongside the COBIT framework and the ISO/IEC 17799 standard when formulating ICT risk management. Furthermore, the Basel II accord provides operational process to specifically manage operational risk. As a result, future studies can utilise this standard to enhance managing operational risk along with the COBIT framework and the ISO/IEC 17799 standard.

Third, the research findings from both the case studies and the survey were based on the direction of organisational communication which included the top-down (the corporate level) and the bottom-up approaches (the operational level). In addition, the scope of the research focused on only the directional level of communication rather than the structure of the control level (strategic, operational or tactical level). The reason is that this research focused on the stipulations of the management buy-in and the operation buy-in when developing the planning regarding ICT risk management in an organisation. The structure of the control level was then not explored. The structure of the control level helps provide clear role and responsibilities of all staff levels to control and manage ICT risk. Therefore, the structure of the control level in an organisation also needs to consider when exploring successful ICT risk management.

Fourth, this research empirically explored success factors of ICT risk management based on ICT governance and IS governance. However, corporate governance of ICT (ISO/IEC 38500 standard) was not a focus in this research because the new ISO/IEC 38500 standard for ICT corporate governance was only recently released in June 2008 by which time this research was near completion. Thus, it was important to recognise the omission of this standard as a limitation of this research. The reason is that the ISO/IEC 38500 standard is a major focus for dealing with ICT risk management in organisations. This standard is targeted at the highest level of ICT governance and IS governance when planning the ICT risk management process.

Fifth, this research empirically explored success factors of ICT risk management based on the COBIT framework. However, The Risk IT Practitioner Guide (the Risk Management Standard of ISACA using COBIT and Val IT standard) was not a focus in this research because this standard was also recently released in 2009 by which time this research was near completion. Thus, it was important to recognise the omission of this standard as a limitation of this research. The reason is that the Risk IT Practitioner Guide is a major focus for dealing with ICT risk management in organisations. Additionally, this standard provides the Risk IT framework that describes a detailed process model for the management of IT-related risk.

Sixth, the validation of the relationships amongst six dimensions (organisational policy, human resources management planning, organisational security, management of ICT resources, the corporate level plan and the operational level plan) in the conceptual model generated from multiple case studies was not validated. The reason was because the statistical results in the survey indicated that the effective management of staff and their behaviour, the effective management of information security and the effective planning of ICT risk management at both the corporate and the operational levels were merged as they shared structural similarities. Therefore, the combination of four dimensions in this research limited the ability to validate the relationships amongst them. The research then focused on validating the overall model rather than the individual pathways.

Finally, since the COBIT framework (i.e. ICT governance) and the ISO/IEC 17799 standard (i.e. IS management) cover different areas, the question might be raised as to why the researcher used both to supplement the organisational plan at the governance level. In response, the primary aim of this research necessitated that focusing on the governance aspect alone would be insufficient; an organisation should consider the information security factor at the governance level or in governing bodies.

8.6 Suggestions for future research

This research explored several factors regarding successful ICT risk management. However, detailed consideration of other factors that might influence successful ICT risk management were beyond the scope of this research. The COSO[8] framework was recommended for an investigation of corporate governance planning in relation to setting ICT direction as ICT governance. Therefore, future research might explore how corporate governance based on the COSO framework can help organisations deal with internal control and audits in order to prevent and avoid the occurrence of risk, particularly regarding business risk in ICT processes.

[8] The Committee of Sponsoring Organizations of the Treadway Commissions (COSO) (1992) has published an internal control framework as a method of corporate governance to provide guidance on the internal control elements required by organisations. Internal control components consist of the control environment, risk assessment, control activities, information, and communication and monitoring (COSO 1992).Internal control is defined as the mechanisms used by organisational directors, management and other personnel to provide reasonable assurance for achieving organisational strategies and objectives (COSO 1992; Pathak 2005). Pathak (2005) further adds that having proper internal control risk management is needed to support work effectively, while IIA (2004, p. 6) argues that 'internal controls are one way of treating a risk'.

Second, the COSO-ERM[9] framework was suggested as a useful tool for preparing the fundamental risk management plan to deal with both business and ICT risks. Future research should consider business risk management as the primary framework before focusing on specific areas such as ICT management.

Third, the ISO/IEC 38500 standard (ISO/IEC 2008) was recommended when considering supplementing ICT risk management in governing bodies at the corporate level. A researcher or a practitioner can use this new standard to explore success factors in order to optimise ICT control and audit for an organisation when dealing with internal control and audit, risk management and ICT risk management at the board and executive management levels.

Fourth, the ITIL framework as ICT service management was proposed to consider third parties and managing ICT service as factors for inclusion in the model of this research, in order to cover all details of ICT risk management planning. Future research should explore success factors based on this framework in order to supplement this research when investigating successful ICT risk management (thus focusing on both the internal and external environments).

Fifth, The Risk IT Practitioner Guide was proposed to assist organisations to set up an IT risk management framework in the enterprise, as well as to enhance existing IT risk management practices. Therefore, this standard is imperative to be investigated along with this research to enhance ICT risk management planning in future research.

Sixth, the findings from the qualitative analysis suggested that the ICT department was required to restructure such that it will take care of both general ICT and ICT security responsibilities. Furthermore, the ICT security function was normally embedded in the ICT department. However, this may not be appropriate because these functions must be responsible for different duties and tasks, and should be able to directly report on their responsibilities to the board and executive management. Therefore, future research should consider the impact of organisational structure in terms of the ICT department and IS department on ICT risk management in organisations.

Lastly, the findings from the quantitative analysis indicated that the effective management and planning of people and their behaviour, the effective management of organisational information security, the effective planning of a corporate plan and the effective planning of a operational plan were of a similar structure statistically. The four constructs were then combined as the statistical analysis suggests. In fact, the four

[9] COSO-ERM is a process affected by an entity's Board of Directors, management and other personnel, applied in a strategy setting and across the enterprise, designed to identify potential events that may affect the entity, to manage risk to be within its risk appetite, and to provide reasonable assurance regarding the achievement of entity objectives (COSO 2004, p. 2). However, COSO-ERM focuses only on business process instead of information technology and/or information security processes.

constructs consisted of two key areas: information security (e.g. managing and planning staff and their behaviour and managing information security), and an enterprise plan (e.g. a corporate plan and an operational plan). Therefore, future research should consider exploring each of these constructs in order to evaluate their impact independently on successful ICT risk management in an organisation. The next section concludes this thesis.

8.7 Conclusion

Over the past decade, it has become increasingly imperative that we explore and seek to understand ICT risk management in organisations. ICT risks persist and threaten to become uncontrollable, according to published reports from the US, UK and Asia on the impact of ICT risk in both the public and private sector organisations. Furthermore, digital communication and processes have assumed critical roles within modern organisations. Especially in Thailand, organisations lack awareness of the potential for ICT risks resulting from the proliferation of digital communication and virtual office automation in recent years. Therefore, this research sought to develop a framework to assist Thai organisations in paying more attention to these negative trends, and to utilise ICT in order to prevent, avoid and mitigate ICT risk as a proactive process.

The subject of ICT risk management in organisations has been introduced in frameworks and standards in the past few years in order to help organisations deal with ICT risk. However, success factors of each framework and standard have been little communicated to organisations. Therefore, this research derived what organisations in Thailand believe contributed to success in ICT risk management for organisations to incorporate into their ICT risk management planning. This research contributed to the field by testing these success factors for to prevent, avoid and mitigate operational, technical and strategic risks related to ICT in organisations through a large scale survey. This research supported the suggestion of Solms (2005a) that information security must be considered at both the corporate and the operational levels. Moreover, this research confirmed the recommendation of the ITGI (2007) that the COBIT framework should be used together with the ISO/IEC 17799 standard to supplement the control objectives of ICT risk management in an organisation. The achievement of this research laid in the integration of the COBIT framework and the ISO/IEC 17799 standard as a two-way approach to successful ICT risk management. While the COBIT framework laid the foundation of the top-down approach to risk management, the ISO/IEC 17799 standard supported bottom-up risk management.

This research failed to reveal the specific relationships amongst dimensions in the conceptual model (organisational policy, human resource management planning,

organisational security, management of ICT resources, the corporate level plan and the operational level plan) derived from the multiple case studies of Thai organisations. In addition, the results indicated that human resource management planning, organisational security, the corporate level plan and the operational level plan must be combined statistically to better explain success in ICT risk management. Nevertheless, the combination of the four dimensions confirmed the suggestion of Solms (2005a) that information security must be monitored and planned at both the corporate level (e.g. senior management) and the operational level (e.g. unit manager or operational manager). This research proposed that new relationships amongst the success factors in the ICT risk management model (SICTRM) be re-examined by practitioners and academics in future research.

This research sought to investigate the current profile of ICT risk management to identify and then model the success elements of ICT risk management in a sample of Thai business organisations. This research supported and confirmed previous research that argues that policy must be structured, first at the board of directors and then at the levels of senior management and operational management, who together must delineate the procedures and practices for dealing with ICT risk management. In dealing with ICT risks, several frameworks and standards have been introduced but ICT risks still persist, therefore, the implication of this research was that we can learn from the Thai organisations that organisations needed to consider the success factors when managing ICT risk. This research proposed that three main success factors affect ICT risk management in Thai organisations. Firstly, the effective organisational policy helped the Thai organisations to plan the effective management of ICT resources and the effective planning of enterprise information security. Secondly, the effective management of ICT resources facilitated the planning of enterprise information security to achieve successful ICT risk management planning. In addition, the survey results have shown that effective organisational policy was the main influence on the management of ICT resources and the planning of enterprise information security. All three success factors complement each other and were significant together in terms of strategic development (i.e. policy) and strategic implementation (i.e. management direction). Lastly, the effective planning of enterprise information security was shown to be a critical factor that helped an organisation mitigate, prevent and avoid operational, technical and strategic risks related to ICT. All three success factors were initially drawn from both the COBIT framework and the ISO/IEC 17799 standard and were found to positively contribute to successful ICT risk management.

References

Allen, J 2005, *Governing for enterprise security: Network systems survivalability program*, Technical Note Carnegie Mellon University and the Software Engineering Institute (CMU/SEI-2005-TN-023). viewed 9 June 2008, <http://www.cert.org/archive/pdf/05tn023.pdf>.

Anderson, EE & Choobineh, J 2008, 'Enterprise information security strategies', *Computers & Security*, vol. 27, no. 1-2, pp. 22-9.

Anderson, JC & Gerbing, DW 1988, 'Structural equation modeling in practice: A review and recommended two-step approach', *Psychological Bulletin*, vol. 103, no. 3, pp. 411-23.

Asian Human Rights Commission (AHRC) 2007, *'Thailand: Unintelligible computer "law" passed under junta's watch'*, viewed 20 January 2008, <http://www.ahrchk.net/statements/mainfile.php/2007statements/1133>.

Audit Commission 2005, *ICT fraud and abuse 2004*, The Audit Commission for authorities and the National Health Service in England and Wales, England.

Baccarini, D, Salm, G & Love, PE 2004, 'Management of risks in information technology projects', *Industrial Management and Data Systems*, vol. 104, no. 4, pp. 286-95.

Badenhorst, KP & Eloff, JHP 1994, 'TOPM: A formal approach to the optimization of information technology risk management', *Computers and Security*, vol. 13, no. 5, p. 435.

Bae, B, Epps, RW & Gwathmey, SS 2003, 'Internal control issues: The case of changes to information processes', *Information Systems Control Journal*, vol. 4, pp. 44-6.

Baert, P 2005, *Philosophy of the social sciences: Towards pragmatism*, Polity, Cambridge, UK.

Bandalos, DL & Finney, SJ 2001, 'Item parceling issues in structural equation modeling', in GA Marcoulides & RE Schumacker (eds), *New developments and techniques in*

structural equation modeling, Lawrence Erlbaum Associates Publishers, NJ. pp. 269-296.

Bandyopadhyay, K, Mykytyn, PP & Mykytyn, K 1999, 'A framework for integrated risk management in information technology', *Management Decision*, vol. 37, no. 5, pp. 437-45.

Bank for International Settlements (Basel) 2005, *International convergence of capital measurement and capital standards*, Basel, Switzerland.

Baumgartner, H & Homburg, C 1996, 'Applications of structural equation modeling in marketing and consumer research: A review', *International Journal of Research in Marketing*, vol. 13, no. 2, pp. 139-61.

Benaroch, M, Lichtenstein, Y & Robinson, K 2006, 'Real options in IT risk management: An empirical validation of risk-option relationships', *MIS Quarterly*, vol. 30, no. 2, pp. 827–64.

Benbasat, I, Goldstein, DK & Mead, M 1987, 'The case research strategy in studies of information systems', *MIS Quarterly*, vol. 11, no. 3, pp. 369-86.

Bentler, PM & Bonett, DG 1980, 'Significance tests and goodness of fit in the analysis of covariance structures', *Psychological Bulletin*, vol. 88, no. 3, pp. 588-606.

Bentler, PM & Chou, CP 1987, 'Practical issues in structural modeling', *Sociological Methods & Research*, vol. 16, no. 1, p. 78.

Berry, AJ, Coad, AF, Harris, EP, Otley, DT & Stringer, C 2009, 'Emerging themes in management control: A review of recent literature', *The British Accounting Review*, vol. 41, no. 1, pp. 2-20.

Bodnar, GH 2003, 'IT Governance', *Internal Auditing-Boston-Warren Gorham and Lamont Incorporated*, vol. 18, no. 3, pp. 27-32.

---- Bodnar, GH 2006, 'What's new in CobiT 4.0', *Internal Auditing-Boston-Warren Gorham and Lamont Incorporated*, vol. 21, no. 4, p. 37.

Bojanc, R & Jerman-Blazic, B 2008, 'Towards a standard approach for quantifying an ICT security investment', *Computer Standards & Interfaces*, vol. 30, no. 4, pp. 216-22.

Bollen, KA 1989, *Structural equations with latent variables*, Wiley series in probability and mathematical statistics. Applied probability and statistics, Wiley, New York.

Boritz, JE 2005, 'IS practitioners' views on core concepts of information integrity', *International Journal of Accounting Information Systems*, vol. 6, no. 4, pp. 260-79.

Braun, V & Clarke, V 2006, 'Using thematic analysis in psychology', *Qualitative research in Psychology*, vol. 3, no. 2, pp. 77-101.

Broderick, JS 2006, 'ISMS, security standards and security regulations', *Information Security Technical Report*, vol. 11, no. 1, pp. 26-31.

Brown, W & Nasuti, F 2005, 'Sarbanes—Oxley and enterprise security: IT governance—What it takes to get the job done', *EDPACS*, vol. 33, no. 2, pp. 1-20.

Bryman, A 2008, *Social research methods*, 3rd edn, Oxford University Press, Oxford; New York.

Buchanan, S & Gibb, F 2007, 'The information audit: Role and scope', *International Journal of Information Management*, vol. 27, no. 3, pp. 159-72.

Buckby, S, Best, P & Stewart, J 2005, 'The role of boards in reviewing information technology governance (ITG) as part of organizational control environment assessments', *Proceedings 2005 IT Governance International Conference*, Auckland, New Zealand.

---- 2009, *'The current state of information technology governance literature'*, in A Cater-Steel (ed.), Information technology governance and service management: Frameworks and adaptations, Information Science Reference, Hershey, pp. xxiii, 495.

Byrd, TA, Sankar, CS & McCreary, JD 1995, 'The strategic risks of implementing global information technology', *Information Strategy*: *The Executive's Journal*, vol. 12, no. 1, p. 39.

Byrne, B 1994, 'Testing for the factorial validity, replication, and invariance of a measuring instrument: A paradigmatic application based on the Maslach Burnout Inventory', *Multivariate Behavioral Research*, vol. 29, no. 3, pp. 289-311.

Byrne, BM 2001, *Structural equation modeling with AMOS : Basic concepts, applications, and programming*, Multivariate applications book series, Lawrence Erlbaum Associates, Mahwah, NJ.

Calder, A & Watkins, S 2005, *IT governance: A manager's guide to data security and BS 7799/ISO/IEC 17799*, 3rd edn, Kogan Page Limited, London; Sterling, VA.

---- 2008, *IT governance: A manager's guide to data security and ISO 27001/ISO 27002*, 4th edn, Kogan Page Limited, London; Philadelphia.

Calderon, TG & Dishovska, M 2005, 'Transitioning from disaster recovery management to business continuity management', *Internal Auditing*, vol. 20, no. 2, p. 21.

Campbell, DT & Fiske, DW 1959, 'Convergent and discriminant validation by the multitrait-multimethod matrix', *Psychological Bulletin*, vol. 56, no. 2, pp. 81-105.

Capuder, L 2004, 'ISO-17799–Standard for information security: A welcome boon for security management and audit', *EDPACS*, vol. 31, no. 11, pp. 1-10.

Caralli, RA, Allen, JH, Stevens, JF, Willke, BJ & Wilson, WR 2004, *'Managing for enterprise security'*, Technical Note Carnegie Mellon University and the Software Engineering Institute (CMU/SEI-2004-TN-046). viewed 9 June 2007, <http://www.sei.cmu.edu/publications/documents/04.reports/04tn046.html>.

Carlson, M & Mulaik, SA 1993, 'Trait ratings from descriptions of behavior as mediated by components of meaning', *Multivariate Behavioral Research*, vol. 28, no. 1, pp. 111-59.

Carmines, EG & McIver, JP 1981, 'Analyzing models with unobserved variables: Analysis of covariance structures', in GW Bohrnstedt & EF Borgatta (eds), *Social measurement: Current issues*, Sage, Beverly Hills, CA, pp. 61-73.

Carnaghan, C 2006, 'Business process modeling approaches in the context of process level audit risk assessment: An analysis and comparison', *International Journal of Accounting Information Systems*, vol. 7, no. 2, pp. 170-204.

Cattell, RB & Burdsal Jr, CA 1975, 'The radial parcel double factoring design: A solution to the item-vs-parcel controversy', *Multivariate Behavioral Research*, vol. 10, no. 2, pp. 165-79.

Cavana, RY, Sekaran, U & Delahaye, BL 2001, *Applied business research: Qualitative and quantitative methods*, John Wiley & Sons Australia, Milton, Qld.

Cavaye, ALM 1996, 'Case study research: A multi-faceted research approach for IS', *Information Systems Journal*, vol. 6, no. 3, pp. 227-42.

Center for Technology in government 2007, *'Making smart IT choices: Understanding value and risk in government IT investment'*, vol. 2007, no. 10 January, <http://www.ctg.albany.edu/publications/guides/smartit2?chapter=3>.

Cha, SC, Juo, PW, Liu, LT & Chen, WN 2008, 'RiskPatrol: A risk management system considering the integration risk management with business continuity processes', *Proceedings of IEEE International Conference on Intelligence and Security Informatics 2008*, ISI 2008, Taiwan.

Christensen, T, Lægreid, P, Roness, PG & Rovik, KA 2007, *Organization Theory and the Public Sector: Instrument, culture and myth*, Routledge, Taylor & Francis Group, <http://www.RMIT.eblib.com.au/EBLWeb/patron?target=patron&extendedid=P_325155_0&>.

Ciarli, T & Rabellotti, R 2007, 'ICTs in industrial districts: An empirical analysis on adoption, use and impact in the Biella Textile District', *Industry and Innovation*, vol. 14, no. 3, pp. 277-303.

Ciborra, C 2006, 'Imbrication of representations: Risk and digital technologies', *Journal of Management Studies*, vol. 43, no. 6, p. 1339.

Cicchetti, DV, Shoinralter, D & Tyrer, PJ 1985, 'The effect of number of rating scale categories on levels of interrater reliability: A Monte Carlo investigation', *Applied Psychological Measurement*, vol. 9, no. 1, pp. 31-6.

Clementi, S & Carvalho, TCMB 2007, 'Methodology for IT governance assessment and design', in *IFIP International Federation for Information Processing*, Springer, Boston, vol. 226, pp. 189-202.

Colbert, J & Bowen, PL 1996, 'A comparison of internal controls: COBIT, SAC, COSO and SAS 55/78', *IS Audit & Control Journal*, vol. 4, pp. 26-35.

Coles, RS & Moulton, R 2003, 'Operationalizing IT risk management', *Computers & Security*, vol. 22, no. 6, pp. 487-93.

Committee of Sponsoring Organisations of the Treadway Commission (COSO) 2004, '*Enterprise risk management-Integrated framework: Executive summary'*, view 15 June 2007, <http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf>.

Conway, JM & Huffcutt, AI 2003, 'A review and evaluation of exploratory factor analysis practices in organizational research', *Organizational Research Methods*, vol. 6, no. 2, pp. 147-68.

Cook, JD 1981, *The experience of work: A compendium and review of 249 measures and their use*, Academic Press, San Diego.

Cox III, EP 1980, 'The optimal number of response alternatives for a scale: A review', *Journal of Marketing Research*, vol. 17, no. 4, pp. 407-22.

Creswell, JW & Plano Clark, VL 2007, *Designing and conducting mixed methods research*, SAGE Publications, Thousand Oaks, California.

Cronbach, LJ & Meehl, P 1955, 'Construct validity in psychological tests', *Psychological Bulletin*, vol. 52, no. 4, pp. 281-302.

Cronbach, LJ 1951, 'Coefficient alpha and the internal structure of tests', *Psychometrika*, vol. 16, no. 3, pp. 297-334.

Damianides, M 2005, 'Sarbanes-Oxley and IT governance: New guidance on IT control and compliance', *Information Systems Management*, vol. 22, no. 1, pp. 77-85.

Darke, P, Shanks, G & Broadbent, M 1998, 'Successfully completing case study research: Combining rigour, relevance and pragmatism', *Information Systems Journal*, vol. 8, no. 4, pp. 273-89.

Dhillon, G & Backhouse, J 1996, 'Risks in the use of information technology within organizations', *International Journal of Information Management*, vol. 16, no. 1, pp. 65-74.

Dillman, DA 2007, *Mail and internet surveys: The tailored design method*, 2nd edn, 2007 update with new internet, visual, and mixed-mode guide. Wiley, Hoboken, NJ.

Earl, MJ 1989, *Management strategies for information technology*, Business information technology series, Prentice Hall, New York.

Eisenhardt, K 1989, 'Building theories from case study research', *Academy of Management Review*, vol. 14, no. 4, pp. 532-50.

Elieson, B 2006, *'Construction of an IT Risk Framework'*, IT Governance Institute (ITGI), viewed 15 June 2007, <http://www.isaca.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=33595>.

Eloff, JHP & Eloff, M 2003, 'Information security management: A new paradigm', *Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists (SAICSIT) on Enablement through technology*.

Enders, CK & Bandalos, DL 1999, 'The effects of heterogeneous item distributions on reliability', *Applied Measurement in Education*, vol. 12, no. 2, pp. 133-50.

Fabrigar, LR, Wegener, DT, MacCallum, RC & Strahan, EJ 1999, 'Evaluating the use of exploratory factor analysis in psychological research', *Psychological Methods*, vol. 4, no. 3, pp. 272-99.

Farrar, JH 2005, *Corporate governance: Theories, principles, and practice*, 2nd edn, Oxford University Press, South Melbourne, Victoria.

Figg, J 1999, 'New guidance released on IT risk management', *Internal Auditor*, vol. 56, no. 3, p. 16.

Finn, RH 1972, 'Effects of some variations in rating scale characteristics on the means and reliabilities of ratings', *Educational and Psychological Measurement*, vol. 32, pp. 255-65.

Finne, T 2000, 'Information systems risk management: Key concepts and business processes', *Computers & Security*, vol. 19, no. 3, pp. 234-42.

Fletcher, M 2006, *Five domains of information technology governance for consideration by boards of directors*, Applied Information Management Master Degree, Project, University of Oregon.

Flowerday, S & Solms, VR 2005, 'Real-time information integrity= system integrity+ data integrity+ continuous assurances', *Computers & Security*, vol. 24, no. 8, pp. 604-13.

Fornell, C & Larcker, DF 1981, 'Evaluating structural equation models with unobservable variables and measurement error', *Journal of Marketing Research*, vol. 18, no. 1, pp. 39-50.

Frohlich, MT 2002, 'Techniques for improving response rates in OM survey research', *Journal of Operations Management*, vol. 20, no. 1, pp. 53-62.

Gable, GG 1994, 'Integrating case study and survey research methods: An example in information systems', *European Journal of Information Systems*, vol. 3, no. 2, pp. 112-26.

Gallegos, F, Senft, S, Manson, DP & Gonzales, C 2004, *Information technology control and audit*, Auerback Publications, Florida.

Garson, DG 2009, *From statnotes: Topics in multivariate analysis*, viewed 04 June 2009, <http://faculty.chass.ncsu.edu/garson/pa765/statnote.htm>.

Gelinas, UJ, Sutton, SG & Hunton, JE 2005, *Accounting information systems*, 6th edn, Thomson South-Western, Mason, Ohio.

Gerber, M & Solms, VR 2005, 'Management of risk in the information age', *Computers & Security*, vol. 24, no. 1, pp. 16-30.

Gerbing, DW & Anderson, JC 1985, 'The effects of sampling error and model characteristics on parameter estimation for maximum likelihood confirmatory factor analysis', *Multivariate Behavioral Research*, vol. 20, no. 3, pp. 255-71.

Gerke, L & Ridley, G 2006, 'Towards an abbreviated COBIT framework for use in an Australian State Public Sector', *Australasian Conference on Information Systems (ACIS) Proceedings*, Adelaide, Paper 83. <http://aisel.aisnet.org/acis2006/83>.

Glaser, BG & Strauss, AL 1967, *The discovery of grounded theory*, Aldine, Chicago.

---- 1977, *The discovery of grounded theory: Strategies for qualitative research*, Aldine, Chicago.

Gordon, LA, Loeb, MP, Lucyshyn, W & Sohail, T 2006, 'The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities', *Journal of Accounting and Public Policy*, vol. 25, no. 5, pp. 503-30.

Gordon, TE 2001, 'A confirmatory analysis of the wechsler adult intelligence scale-third edition: Is the verbal/performance discrepancy justified?', *Practical Assessment, Research & Evaluation*, vol. 7, no. 22, viewed March 1, 2009 http://PAREonline.net/getvn.asp?v=7&n=22.

Gorsuch, RL 1983, *Factor analysis*, 2nd edn, Lawrence Erlbaum Associates, Hillsdale, New Jersey.

Gotterbarn, D 2009, 'ICT governance and what to do about the toothless tiger(s): Professional organisations and codes of ethics', *Australasian Journal of Information Systems*, vol. 16, no. 1, pp.165-184.

Grinnell, RM 1985, *Social work research and evaluation*, 2nd edn, FE Peacock Publishers, Itasca, Illinois.

Groves, S 2003, 'The unlikely heroes of cyber security', *Information Management Journal*, vol. 37, no. 3, pp. 34-42.

Guldentops, E, Van Grembergen, W & De Haes, S 2002, 'Control and governance maturity survey: Establishing a reference benchmark and a self-assessment tool', *Information Systems Control Journal*, vol. 6, pp. 32-35.

Hair, JF, Black, WC, Babin, BJ, Anderson, RE & Tatham, RL 2006, *Multivariate data analysis*, 6th edn, Pearson Prentice Hall, Upper Saddle River, New Jersey.

Hall, RJ, Snell, AF & Foust, MS 1999, 'Item parceling strategies in SEM: Investigating the subtle effects of unmodeled secondary constructs', *Organizational Research Methods*, vol. 2, no. 3, pp. 233-56.

Hanson, WE, Creswell, JW, Plano Clark, VL, Petska, KS & Creswell, JD 2005, 'Mixed methods research designs in counseling psychology', *Journal of Counseling Psychology*, vol. 52, no. 2, pp. 224-35.

Hardy, G 2006, 'Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges', *Information Security Technical Report*, vol. 11, no. 1, pp. 55-61.

Harris, BA 2007, *'A compilation of survey response options'*, viewed 20 January 2007, <http://dataguru.org/ref/survey/responseoptions.asp>.

Hawkins, KW, Alhajjaj, S & Kelley, SS 2003, 'Using CobiT to secure information assets', *The Journal of Government Financial Management*, vol. 52, no. 2, pp. 22-33.

Haworth, DA & Pietron, LR 2006, 'Sarbanes-Oxley: Achieving compliance by starting with ISO/IEC 17799', *Information Systems Management*, vol. 23, no. 1, pp. 73-87.

Hayat, Z, Reeve, J & Boutle, C 2007, 'Ubiquitous security for ubiquitous computing', *Information Security Technical Report*, vol. 12, no. 3, pp. 172-8.

Hermanson, DR, Hill, MC & Ivancevich, DM 2000, 'Information Technology related activities of internal auditors', *Journal of Information Systems*, vol. 14, pp. 39-55.

Hilton, J 2009, 'Improving the secure management of personal data: Privacy on-line information security important, but it's not easy', *Information Security Technical Report*, vol. 14, no. 3, pp. 124-30.

Hinton, M 2006, *Introducing information management : The business approach*, Elsevier Butterworth-Heinemann, Amsterdam ; Boston.

Hoelter, JW 1983, 'The analysis of covariance structures: Goodness-of-fit indices', *Sociological Methods & Research*, vol. 11, no. 3, pp. 325-44.

Holmes-Smith, P 2007, *An applied introductory course in structural equation modelling using AMOS*, School Research Evaluation and Measurement Services (SREAMS), Melbourne.

Holzmann, R & Jorgensen, S 2001, 'Social risk management: A new conceptual framework for social protection, and beyond', *International Tax and Public Finance*, vol. 8, no. 4, pp. 529-56.

Hooper, D, Coughlan, J & Mullen, MR 2008, 'Structural equation modelling: Guidelines for determining model fit', *The Electronic Journal of Business Research Methods*, vol. 6, no. 1, pp. 53-60.

Hu, L & Bentler, PM 1998, 'Fit indices in covariance structure modeling: Sensitivity to underparameterized model misspecification', *Psychological Methods*, vol. 3, no. 4, pp. 424-53.

Hughes, G 2006a, 'Five steps to IT risk management best practices', *Risk Management*, vol. 53, no. 7, p. 34.

---- 2006b, *'Managing risk in the storage environment: the realities of risk'*, viewed 8 Febuary 2007, <http://www.thefreelibrary.com/Managingriskinthestorageenvironment:therealitiesofrisk.-a0147748651>.

Huissoud, M (2005) IT self-assessment project, current results and next steps, *Presentation to EUROSAI IT working group*, Cypress, 14 February, 2005.

Iijima, T & Curtis, J 2004, 'Need to justify IT security? Measure your risk!'*, Journal of Corporate Accounting & Finance*, vol. 15, no. 5, pp. 47-51.

The Information System Audit and Control Association (ISACA) Information System Audit and Control Association (ISACA) 2007, *'Sarbanes-Oxley: New guidance on IT control and compliance'*, viewed 15 June 2007, <http://www.isaca.org/Template.cfm?Section=Press_Releases1&CONTENTID=9809&TEMPLATE=/ContentManagement/ContentDisplay.cfm>.

Information System Audit and Control Association (ISACA) 2009, *'The Risk IT Practitioner Guide: Risk Universe, Appetite and Tolerance, Risk Awareness, Communication and Reporting, Expressing and Describing Risk, Risk Scenarios, Risk Responses and Prioritisation Using COBIT and Val IT',* viewed 18 September 2010, <http://www.isaca.org/Knowledge-Center/Research/Documents/RiskIT_PG_30June2010_Research.pdf>

---- 2005, *Information Technology Controls*, viewed 21 October 2008, <http://www.theiia.org//guidance/technology/gtag/gtag1/?search=Information%20technology%20controls>.

Institue of Internal Auditors (IIA) 2004, *'The role of internal auditing in enterprise-wide risk management'*, view 15 June 2007, <http://www.iia.org.au/_webapp_263859/The_Role_of_Internal_Auditing_in_Enterprise-wide_Risk_Management>.

---- 1993, *System auditibility and control report*, IIA, Altamonte, Florida.

International Federation of Accountants (IFAC) 1995, *Information technology in the accounting curriculum, education guideline*, IFAC, New York.

International Organization for Standardization (ISO) & The International Electrotechnical Commission (IEC) 2005, *Information technology - security techniques - code of practice for information security management*, 2nd edn, International standard; ISO/IEC 17799:2005(E), ISO/IEC, Geneva.

---- 2008, *Corporate governance of information technology = Gouvernance des technologies de l'information par l'enterprise, International standard*; ISO/IEC 38500, ISO/IEC, Geneva.

Irani, Z, Themistocleous, M & Love, PED 2003, 'The impact of enterprise application integration on information system lifecycles', *Information & Management*, vol. 41, no. 2, pp. 177-87.

ISM3 Consortium 2007, *Information security management maturity model, ISM3*, viewed 9 June 2007, <www.ism3.com/cmmicobitism3.php>.

ISO/IEC 17799 Compliance Associates 2002, *'Where to find resources, expertise and information for ISO/IEC 17799'*, viewed 26 June 2007, <http://17799.macassistant.com/riskanalysis.htm>.

Israel, DG 2003, *'Determining sample size'*, PEOD6, the Agricultural Education and Communication Department, Florida Cooperative Extension Service, Institute of Food and Agricultural Sciences, University of Florida, viewed 10 September 2008, <http://edis.ifas.ufl.edu/pd006>.

IT Governance Institute (ITGI) & The Office of Government Commerce (OGC) 2005, *Aligning COBIT, ITIL, and ISO/IEC 17799 for business benefit: Management summary, A management briefing from ITGI and OGC*, ITGI & OGC, England.

---- 2008, *Aligning COBIT 4.1, ITIL v3 and ISO/IEC 27002 for business benefit, A management briefing from ITGI and OGC*, ITGI & OGC, England.

The IT Governance Institute (ITGI) 2005, *Information risks: Whose business are they?*, IT governance domain practices and competencies, ITGI, Illinois.

---- 2006a, COBIT mapping: *Mapping of ISO/IEC 17799:2005 with COBIT 4.0, ITGI*, Illinois.

---- 2006b, *Information security governance: Guidance for boards of directors and executive management*, 2nd edn, ITGI, Illinois.

---- 2007, *COBIT 4.1: Framework, control objectives, management guidelines and maturity models*, ITGI, Illinois.

Jaccard, J & Wan, CK 1996, *LISREL approaches to interaction effects in multiple regression*, Sage university papers series. Quantitative applications in the social sciences; no. 07-114, Sage Publications, Thousand Oaks, California.

Johnson, S, Boone, P, Breach, A, & Friedman, E 2000, 'Corporate governance in the Asian Financial Crisis', *Journal of Financial Economics*, vol. 58, no.1-2, pp. 141-186

Jordan, E & Silcock, L 2005, *Beating IT risks*, John Wiley & Sons, Chichester.

Joreskog, KG & Sorbom, D 1989, *'Lisrel 7 user's reference guide'*, Mooresville, IN, Scientific Software.

Josephson, J 1996, *Abductive inference: Computation, philosophy, technology*, Cambridge University Press.

Kaplan, B & Duchon, D 1988, 'Combining qualitative and quantitative methods in information systems research: A case study', *MIS Quarterly*, vol. 12, no. 4, pp. 571-86.

Kaplan, D 2000, *Structural equation modeling: Foundations and extensions*, Sage Publications, Thousand Oaks, California.

Kaplan, RS & Norton, DP 1993, 'Putting the balanced scorecard to work', *Harvard Business Review*, September-October, pp. 134-47.

---- 2007, 'Using the balanced scorecard as a Strategic Management System', Harvard Business Review, *Managing for the long term*, pp. 1-14.

Karabacak, B & Sogukpinar, I 2006, 'A quantitative method for ISO/IEC 17799 gap analysis', *Computers & Security*, vol. 25, no. 6, pp. 413-9.

Kenning, MJ 2001, 'Security management standard—ISO/IEC 17799/BS 7799', *BT Technology Journal*, vol. 19, no. 3, pp. 132-6.

Kenny, S 2004, *'Assuring data privacy compliance*, ' Information Systems Control Journal, Information Systems Audit and Control Association (ISACA), viewed 8 June 2007,

<http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=21323&TEMPLATE=/ContentManagement/ContentDisplay.cfm>.

Khan, K 2006, 'How IT governance is changing', *Journal of Corporate Accounting & Finance*, vol. 17, no. 5, pp. 21-5.

Klein, HK & Myers, MD 1999, 'A set of principles for conducting and evaluating interpretive field studies in information systems', *MIS Quarterly*, vol. 23, no. 1, pp. 67-93.

Kline, RB 1998, *Principles and practice of structural equation modeling: Methodology in the social sciences*, Guilford Press, New York.

---- 2005, *Principles and practice of structural equation modeling*, 2nd edn, Methodology in the social sciences, Guilford Press, New York.

Koanantakool, T 2000, *'Thailand information technology environment 2000'*, National Electronics and Computer Technology Center of Thailand (NECTEC), Ministry of Science, Technology and Environment, Thailand, viewed 14 June 2009, <http://www.docstoc.com/docs/18367765/THAILAND-Information-Technology-Environment-2000>.

Korac-Kakabadse, N & Kakabadse, A 2001, 'IS/IT governance: Need for an integrated model', *Corporate Governance*, vol. 1, no. 4, pp. 9-11.

Krippendorff, K 2004, *Content analysis: An introduction to its methodology*, 2nd edn, Sage, Thousand Oaks, California.

Ksiezopolski, B & Kotulski, Z 2007, 'Adaptable security mechanism for dynamic environments', *Computers & Security*, vol. 26, no. 3, pp. 246-55.

Ladan, SH, Yari, A & Khodabandeh, H 2006, *'Combination of information security standards to cover national requirements'*, World Academy of Science, Engineering and Technology, vol. 13, viewed 7 June 2009, <http://www.waset.org/journals/waset/v13/v13-30.pdf>.

Lainhart IV, JW 2000, 'COBIT: A methodology for managing and controlling information and information technology risks and vulnerabilities', *Journal of Information Systems*, vol. 14, pp. 21-5.

---- 2001a, 'An IT assurance framework for the future', *Ohio CPA Journal*, vol. 60, no. 1, p. 19.

---- 2001b, 'Why IT governance is a top management issue', *Journal of Corporate Accounting & Finance*, vol. 11, no. 5, pp. 33-40.

Lee, AS 1991, 'Integrating positivist and interpretive approaches to organizational research', *Organization science*, vol. 2, no. 4, pp. 342-65.

Leung, P, Cooper, BJ & Robertson, PT 2003, *The role of internal audit in corporate governance & management*, School of Accounting and Law, RMIT University, Institute of Internal Auditors (Australia), Melbourne.

Levine, R 2004, 'Risk management systems: Understanding the need', *Information Systems Management*, vol. 21, no. 2, p. 31.

Li, X & Johnson, JD 2002, 'Evaluate IT investment opportunities using real options theory', *Information Resources Management Journal*, vol. 15, no. 3, pp. 32-47.

Lientz, BP & Larssen, L 2004, *Manage IT as a business: How to achieve alignment and add value to the company*, Elsevier Butterworth Heinemann, Amsterdam; Boston.

---- 2006, *Risk management for IT projects : How to deal with over 150 issues and risks*, Elsevier/Butterworth-Heinemann, Amsterdam; Boston.

Little, TD, Cunningham, WA, Shahar, G & Widaman, KF 2002, 'To parcel or not to parcel: Exploring the question, weighing the merits', *Structural Equation Modeling*, vol. 9, no. 2, pp. 151-73.

Liu, Q & Ridley, G 2005, 'IT control in the Australian public sector: An international comparison', *Proceedings of the 13th European Conference of Information Systems*, Regensburg, Germany.

Lloyd, I 2000, *Information technology law*, 5th edn, Butterworths, London.

Longstaff, TA, Chittister, C, Pethia, R & Haimes, YY 2000, 'Are we forgetting the risks of information technology?', *Computer*, vol. 33, no. 12, pp. 43-51.

Luborsky, MR 1994, 'The identification of themes and patterns', in JF Gubrium & A Sankar (eds), *Qualitative methods in aging research*, Sage Publications, Thousand Oaks, CA.

Luftman, JN, Lewis, PR & Oldach, SH 1993, 'Transforming the enterprise: The alignment of business and information technology strategies', *IBM Systems Journal*, vol. 32, no. 1, pp. 198-221.

Mansell, R 1999, 'Information and communication technologies for development: Assessing the potential and the risks', *Telecommunications Policy*, vol. 23, no. 1, pp. 35-50.

Mardia, K 1970, 'Measures of multivariate skewness and kurtosis with applications', *Biometrika*, vol. 57, no. 3, pp. 519-30.

Marsh, HW, Balla, JR & McDonald, RP 1988, 'Goodness-of-fit indexes in confirmatory factor analysis: The effect of sample size', *Psychological Bulletin*, vol. 103, no. 3, pp. 391-410.

Martin, A 2003, 'What drives the configuration of information technology projects? Exploratory research in 10 organizations', *Journal of Information Technology*, vol. 18, no. 1, pp. 1-15.

Martinez, MA, Lasheras, J, Fernandez-Medina, E, Toval, A & Piattini, M 2010, 'A personal data audit method through requirements engineering', *Computer Standards & Interfaces*, vol. In Press, Corrected Proof, doi: 10.1016/j.csi.2010.01.001.

McAdams, AC 2004, 'Security and risk management: A fundamental business issue', *Information Management Journal*, vol. 38, no. 4, pp. 36-45.

McEvoy, N & Whitcombe, A 2002, 'Structured risk analysis'*, in Lecture Notes in Computer Science (LNCS)*, Infrastructure Security, Springer Benlin, Heidelberg, vol. 2437/2002, pp. 88-103.

McGaughey, RE, Snyder, CA & Carr, HH 1994, 'Implementing information technology for competitive advantage: Risk management issues', *Information & Management*, vol. 26, no. 5, pp. 273-80.

McLeod, R & Schell, GP 2007, *Management information systems*, 10th edn, Pearson/Prentice Hall, Upper Saddle River, New Jersey.

McNurlin, BC & Sprague, RH 2006, *Information systems management in practice*, 7th edn, Pearson Prentice Hall, Upper Saddle River, NJ.

Mena, C 2002, 'Making security a team effort', *Optimize*, October, pp. 38-44.

Miaoulis, G & Michener, RD 1976, *An introduction to sampling*, Kendall, Dubuque, Iowa.

Milenkovic, I 2008, 'Adapting organisations for role-based access control measures', *Computer Fraud & Security*, vol. 2008, no. 11, pp. 14-8.

Miller, GA 1956, 'The magical number seven, plus or minus two: Some limits on our capacity for processing information', *Psychological Review*, vol. 63, no. 2, pp. 81-97.

Mitton, T 2002, 'A cross-firm analysis of the impact of corporate governance on the East Asian financial crisis', *Journal of Financial Economics*, vol. 64, no. 2, pp. 215-41.

Moeller, RR 2005, *Brink's modern internal auditing*, 6th edn, John Wiley & Sons Inc., Hoboken, NJ.

---- 2007, *COSO enterprise risk management understanding the new integrated ERM framework*, John Wiley & Sons Inc., Hoboken.

Morris, BW & Pushkin, AB 1995, 'Determinants of information systems audit involvement in EDI systems development', *Journal of Information Systems*, vol. 9, no. 2, pp. 111-28.

Mulaik, SA & Millsap, RE 2000, 'Doing the four-step right', *Structural Equation Modeling*, vol. 7, no. 1, pp. 36-73.

Myers, KK & Oetzel, JG 2003, 'Exploring the dimensions of organizational assimilation: Creating and validating a measure', *Communication Quarterly*, vol. 51, no. 4, pp. 438-58.

Myers, MD 1997, 'Qualitative research in information systems', *MIS Quarterly*, vol. 21, no. 2, pp. 241-2. MISQ Discovery, Archival version, June 1997, <http://www.misq.org/discovery/MISQD_isworld/>.

Myler, E & Broadbent, G 2006, 'ISO/IEC 17799: Standard for security', *Information Management Journal*, vol. 40, no. 6, p. 43.

Nasser, F & Takahashi, T 2003, 'The effect of using item parcels on ad hoc goodness-of-fit indexes in confirmatory factor analysis: An example using Sarason's Reactions to Tests', *Applied Measurement in Education*, vol. 16, no. 1, pp. 75-97.

National Electronics and Computer Technology Center (NECTEC) & National Science and Technology Development Agency (NSTDA) 2003, *'Thailand ICT Indicators: moving towards the information society'*, Ministry of Science and Technology, Thailand, viewed 9 June 2007, <http://www.nectec.or.th/2008/pdf/ict_indicators2003.pdf>.

Neuman, WL 2000, *Social research methods: Qualitative and quantitative approaches*, 4th edn, Allyn and Bacon, Boston.

---- 2006, *Social research methods: Qualitative and quantitative approaches*, 6th edn, Pearson/AandB, Boston.

Nunnally, JC & Bernstein, IH 1994, *Psychometric theory*, 3rd edn, McGraw-Hill series in psychology, McGraw-Hill, New York.

Nunnally, JC 1967, *Psychometric theory*, McGraw-Hill series in psychology, McGraw-Hill, New York.

---- 1978, *Psychometric theory*, 2nd edn, McGraw-Hill, New York.

Oaster, TRF 1989, 'Number of alternatives per choice point and stability of Likert-type scales', *Perceptual and Motor Skills*, vol. 68, pp. 549-50.

O'Brien, JA & Marakas, GM 2009, *Management information systems*, 9th edn, McGraw-Hill Irwin, Boston.

Office of Government Commerce (OGC) *'ITIL: The key to managing IT services'*, viewed 20 December 2009, <http://www.itil-officialsite.com/home/home.asp>.

O'Leary-Kelly, SW & Vokurka, RJ 1998, 'The empirical assessment of construct validity', *Journal of Operations Management*, vol. 16, no. 4, pp. 387-405.

Olsson, UH 1979, 'On the robustness of factor analysis against crude classification of the observations', *Multivariate Behavioral Research*, vol. 14, no. 4, pp. 485-500.

Olsson, UH, Foss, T, Troye, SV & Howell, RD 2000, 'The performance of ML, GLS, and WLS estimation in structural equation modeling under conditions of misspecification and nonnormality', *Structural Equation Modeling*, vol. 7, no. 4, pp. 557-95.

Osborne, JW 2008, *Best practices in quantitative methods*, Sage Publications, Thousand Oaks, Calif.

Ousterhout, J, Da Costa, H, Harrison, D, Kunze, J, Kupfer, M & Thompson, J 1985, 'A trace-driven analysis of the UNIX 4.2 BSD file system', *ACM SIGOPS Operating Systems Review*, vol. 19, no. 5, p. 24.

Pathak, J 2005, ‘Risk management internal controls and organizational vulnerabilities’, *Managerial Auditing Journal,* vol. 20, no. 6, pp.569-577.

Pickett, KHS 2005, *The essential handbook of internal auditing*, John Wiley & Son Ltd, Hoboken, New Jersey.

Pinder, P 2006, 'Preparing information security for legal and regulatory compliance (Sarbanes–Oxley and Basel II)', *Information Security Technical Report*, vol. 11, no. 1, pp. 32-8.

Plano Clark, VL, Huddleston-Casas, CA, Churchill, SL, O'Neil Green, D & Garrett, AL 2008, 'Mixed methods approaches in family science research', *Journal of Family Issues*, vol. 29, no. 11, p. 1543.

Poore, RS 2005, 'Information security governance', *EDPACS*, vol. 33, no. 5, p. 1.

Posthumusa, S & Solms, VR 2005, 'IT oversight: An important function of corporate governance', *Computer Fraud & Security*, vol. 2005, no. 6, pp. 11-7.

Ravenel, JP 2006, 'Effective Operational Security Metrics', *EDPACS*, vol. 33, no. 12, pp. 10-9.

Ridley, G, Young, J & Carroll, P 2004, 'COBIT and its utilization: A framework from the literature', *Proceedings of the 37th Hawaii International Conference on System Sciences*, Hawaii.

Rife, RC 1994, 'Software piracy', *Proceedings of NORTHCON '94*.

Robinson, N 2005, 'IT excellence starts with governance', *Journal of Investment Compliance*, vol. 6, no. 3, pp. 45-9.

Ruddock, L 2006, 'ICT in the construction sector: Computing the economic benefits', *International Journal of Strategic Property Management*, vol. 10, no. 1, pp. 39-50.

Saint-Germain, R 2005, 'Information security management best practice based on ISO/IEC 17799', *Information Management Journal*, vol. 39, no. 4, p. 60.

Sarens, G & De Beelde, I 2006, 'Internal auditor's perception about their role in risk management', *Managerial Auditing Journal*, vol. 21, no. 1, pp. 63-80.

Satanasathaporn, S 2007, *'Thailand digital opportunities'*, The Association of Thai ICT Industry (ATCI), viewed 10 November 2009, <www.dof.or.kr/pdf/Thailand%5BPPT%5D.pdf>.

Saunders, M, Thornhill, A & Lewis, P 2003, *Research methods for business students*, 3rd edn, Prentice Hall, Upper Saddle River, NJ.

---- 2007, *Research methods for business students*, 4th edn, Pearson Prentice Hall Financial Times, Harlow, Essex, England.

Scapens, R 1990, 'Researching management accounting practice: The role of case study methods', *The British Accounting Review*, vol. 22, no. 3, pp. 259-81.

Schultz, EE 2007, 'Risks due to convergence of physical security systems and information technology environments', *Information Security Technical Report*, vol. 12, no. 2, pp. 80-4.

Schwab, DP 1980, 'Construct validity in organizational behavior', *Research in Organizational Behavior*, vol. 2, no. 1, pp. 3-43.

Schwarz, A & Hirschheim, R 2003, 'An extended platform logic perspective of IT governance: Managing perceptions and activities of IT', *Journal of Strategic Information Systems*, vol. 12, no. 2, pp. 129-66.

Segars, AH & Grover, V 1996, 'Designing company-wide information systems: Risk factors and coping strategies', *Long Range Planning*, vol. 29, no. 3, pp. 381-92.

Shanks, G, Rouse, A & Arnott, D 1993, 'A review of approaches to research and scholarship in information systems', *Proceedings of the 4th Australian Conference on Information Systems*, Brisbane.

Shendden, P, Ruighaver, T & Ahmad, A 2006, 'Risk management standards: The perception of ease of use', *Proceedings of 5th Annual Security Conference*, Las Vegas, Nevada, USA.

Shenkir, WG & Walker, PL 2006, 'Enterprise risk management and the strategy-risk-focused organization', *Journal of Cost Management*, vol. 20, no. 3, p. 32.

Shortreed, J, Craig, L & McColl, S 2000, *'Benchmark framework for risk management'*, Network for Environmental Risk Assessment and Management (NERAM), viewed 9 June 2007, <http://www.irr-neram.ca/pdf_files/Benchmark2001.pdf>.

Silverman, D 1998, 'Qualitative research: Meanings or practices?', *Information Systems Journal*, vol. 8, no. 1, pp. 3-20.

Siponen, M & Willison, R 2009, 'Information security management standards: Problems and solutions', *Information & Management*, vol. 46, no. 5, pp. 267-70.

Smith, E & Eloff, JHP 2002, 'A prototype for assessing information technology risks in health care', *Computers & Security*, vol. 21, no. 3, pp. 266-84.

Smith, HA & McKeen, JD 2006, 'Developments in practice XXI: IT in the new world of corporate governance reforms', *Communications of the Association for Information Systems*, vol. 17, no. 1, p. 32.

Sohal, AS & Fitzpatrick, P 2002, 'IT governance and management in large Australian organisations', *International Journal of Production Economics*, vol. 75, no. 1-2, pp. 97-112.

Solms, VB & Solms, VR 2005, 'From information security to … business security?', *Computers & Security*, vol. 24, no. 4, pp. 271-3.

Solms, VB 2001, 'Information security: A multidimensional discipline', *Computers & Security*, vol. 20, no. 6, pp. 504-8.

---- 2005a, 'Information Security governance: COBIT or ISO/IEC 17799 or both?', *Computers & Security*, vol. 24, no. 2, pp. 99-104.

---- 2005b, 'Information security governance: Compliance management vs operational management', *Computers & Security*, vol. 24, no. 6, pp. 443-7.

---- 2006a, 'ICT risk governance in a university environment ', *Proceedings of Conference on Information Technology in Tertiary Education (CITTE)*, South Africa, 18–20 September 2006, <http://citte2006.cut.ac.za/res/von%20solms%20risk.pdf>.

---- 2006b, 'Information security: The fourth wave', *Computers & Security*, vol. 25, no. 3, pp. 165-8.

Solms, VR & Solms, VB 2006, 'Information security governance: A model based on the Direct–Control Cycle', *Computers & Security*, vol. 25, no. 6, pp. 408-12.

The Stock Exchange of Thailand (SET) 2008, *'Companies/Securities in focus'*, viewed 1 May 2008, <http://www.set.or.th/set/commonslookup.do>.

The Stock Exchange of Thailand (SET) *'Corporate governance'*, viewed 14 January 2009, <http://www.set.or.th/en/regulations/cg/roles_p1.html>.

Stoneburner, G, Goguen, A & Feringa, A 2002, *'Risk management guide for information technology systems: Recommendations of the National Institute of Standards and Technolgoy (NIST)'*, NIST, SP 800-30, viewed 9 June 2007, <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>.

Straub, D, Boudreau, MC & Gefen, D 2004, 'Validation guidelines for IS positivist research', *Communications of the Association for Information Systems (AIS)*, vol. 13, no. 24, pp. 380-427.

Straub, DW & Welke, RJ 1998, 'Coping with systems risk: Security planning models for management decision making', *MIS Quarterly*, Vol. 22, No. 4, pp. 441-69.

Straub, DW, Goodman, SE & Baskerville, R 2008, *Information security: Policy, processes, and practices*, ME Sharpe, Armonk, New York.

Sweren, SH 2006, 'ISO/IEC 17799: Then, now and in the future ', *Information Systems Control Journal*, vol. 1, <http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=52138&TEMPLATE=/ContentManagement/ContentDisplay.cfm>.

Symonds, PM 1924, 'On the loss of reliability in ratings due to coarseness of the scale', *Journal of Experimental Psychology*, vol. 7, no. 6, pp. 456-61.

Tabachnick, BG & Fidell, LS 2007, *Using multivariate statistics*, 5th [Pearson international] edn, Pearson/Allyn & Bacon, Boston.

Tarantino, A 2008, *Governance, risk and compliance handbook: Technology, finance, environmental and international guidance and best practices*, John Wiley & Sons, Hoboken, New Jersey.

Tashakkori, A & Teddlie, C 2003, *Handbook of mixed methods in social & behavioral research*, SAGE Publications, Thousand Oaks, California.

Teneyuca, D 2001, 'Organizational leader's use of risk management for information technology', *Information Security Technical Report*, vol. 6, no. 3, pp. 54-9.

The UK - The Institute of Risk Management (IRM), The Association of Insurance and Risk Managers (AIRMIC) & ALARM The National Forum for Risk Management in the Public Sector 2002, *A risk management standard, AIRMIC, ALARM and IRM*, viewed 5 January 2009, <http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf>.

Theoharidou, M, Kokolakis, S, Karyda, M & Kiountouzis, E 2005, 'The insider threat to information systems and the effectiveness of ISO17799', *Computers & Security*, vol. 24, no. 6, pp. 472-84.

Thuvasethakul, C & Koanantakool, T 2002, *'National ICT policy in Thailand'*, National Electronics and Computer Technology Center of Thailand (NECTEC), Ministry of Science, Technology and Environment, Thailand, pp. 25-9, viewed 9 June 2007, <http://www.nectec.or.th/users/htk/publish/20020302-National-ICT-Policy-v16-word.pdf>.

Todd, Z, Nerlich, B, McKeown, S & Clarke, DD 2004, *Mixing methods in psychology: The integration of qualitative and quantitative methods in theory and practice*, Psychology Press, New York.

Trites, G 2000, 'Overview of CICA's Information Technology Control Guidelines', *Journal of Information Systems*, vol. 14, pp. 27-32.

---- 2004, 'Director responsibility for IT governance', *International Journal of Accounting Information Systems*, vol. 5, no. 2, pp. 89-99.

Tshinu, SM, Botha, G & Herselman, M 2008, 'An integrated ict management framework for commercial banking organisations in South Africa', *Interdisciplinary Journal of Information, Knowledge, and Management*, vol. 3, pp. 39-53.

Ullman, JB 2001, 'Structural equation modelling', in BG Tabachnick & LS Fidell (eds), *Using multivariate statistics*, 4th edn, Allyn & Bacon, pp. 635-771.

Van Grembergen, W & DeHaes, S 2008, *Implementing information technology governance: Models, practices, and cases*, IGI Publishing, Hershey, PA.

Van Grembergen, W 2000, 'The balanced scorecard and IT governance', *Information Systems Control Journal*, vol. 2, pp. 40-3.

Van Grembergen, W, De Haes, S & Guldentops, E 2004, 'Structures, processes and relational mechanisms for IT governance', in W Van Grembergen (ed.), *Strategies for information technology governance*, Idea Group Publishing, Hershey, pp. 14-36.

Viator, RE & Curtis, MB 1998, 'Computer auditor reliance on automated and non-automated controls as a function of training and experience', *Journal of Information Systems*, vol. 12, no. 1, pp. 19-30.

Vongvipanond, P 2004, *'Thailand's post crisis's institutional change: Corporate restructuring and financial institution risk management'*, Forum on Asian Insolvency Reform, Insolvency Systems and Risk Management in ASIA, OECD, Asian Development Bank, The World Bank, New Delhi, India, 3-5 November 2004.

Walsham, G 2006, 'Doing interpretive research', *European Journal of Information Systems*, vol. 15, no. 3, pp. 320-30.

Ward, J 2005, 'Operational risk and information security need to co-exist if businesses want to effectively manage risk', *Credit Control*, vol. 26, no. 7, p. 18.

Warkentin, M & Johnston, CA 2008, 'IT governance and organisational design for security management', in DW Straub, SE Goodman & R Baskerville (eds), *Information security: Policy, processes, and practices*, ME Sharpe, Armonk, New York, pp. ix, 286.

Warren, JD, Edelson, LW, Parker, XL & Murphy, MA 1996, *Handbook of IT auditing*, 1996 edn, Warren Gorham & Lamont, Boston.

Weill, P & Ross, JW 2004a, *'IT Governance on one page'*, MIT Sloan School of Management, viewed 6 June 2007, <http://web.mit.edu/cisr/working%20papers/cisrwp349.pdf>.

---- 2004b, *IT governance: How top performers manage IT decision rights for superior results*, Harvard Business School Press.

Weitzman, P & Levkoff, S 2000, 'Combining qualitative and quantitative methods in health research with minority elders: Lessons from a study of dementia caregiving', *Field Methods*, vol. 12, no. 3, p. 195.

Westby, JR & Allen, JH 2007, *Governing for enterprise security (GES) implementation guide, Article 3. Enterprise Security Governance Activities*, CERT and CERT Coordination Center, Carnegie Mellon University.

Wheelen, TL & Hunger, JD 2004, *Strategic management and business policy*, 9th edn, Pearson Prentice Hall, Upper Saddle River, NJ.

Whitman, ME & Mattord, HJ 2009, *Principles of information security*, 3rd edn, Thomson Course Technology, Boston, Massachusetts.

Willcocks, L & Griffiths, C 1994, 'Predicting risk of failure in large-scale information technology projects', *Technological Forecasting and Social Change*, vol. 47, no. 2, pp. 205-28.

Willcocks, L, Feeny, D & Olson, N 2006, 'Implementing core IS capabilities: Feeny–Willcocks IT governance and management framework revisited'*, European Management Journal*, vol. 24, no. 1, pp. 28-37.

Wright, S 1923, 'The theory of path coefficients: A reply to Niles' criticism', *Genetics*, vol. 8, no. 3, pp. 239-55.

Yamane, T 1973, *Statistics: An introductory analysis*, 3d edn, Harper & Row, New York.

Yin, RK 1994, *Case study research: Design and methods*, 2nd edn, Applied social research methods series; v. 5, Sage Publications, Thousand Oaks, California.

---- 2003, *Case study research: Design and methods*, 3rd edn, Sage Publications, Thousand Oaks, California.

---- 2009, *Case study research: Design and methods*, 4th edn, Sage Publications, Los Angeles, California.

Yu, C 2002, *'Evaluating Cutoff Criteria of Model Fit Indices for Latent Variable Models with Binary and Continuous Outcomes*', Doctor of Philosophy in Education, thesis, University of California.

Yuan, KH, Bentler, PM & Kano, Y 1997, 'On averaging variables in a confirmatory factor analysis model', *Behaviormetrika*, vol. 24, no. 1, pp. 71-83.

ZDNetAsia 2007, *'Thai banks adopting risk management tools'*, viewed 20 June 2007, <http://www.zdnetasia.com/news/security/0,39044215,62003857,00.htm>.

Appendix A

INTERVIEW

A1. Letter of invitation for the interview

Dear Sir/Madam,

I write to invite you to participate in my research project on the investigation of structured approaches to ICT risk management in organisations. I am a PhD student at the School of Business Information Technology, RMIT University, Melbourne, Australia. My supervisors are Associate Professor Hepu Deng and Professor Brian Corbitt.

ICT risk management is widely used for identifying and managing the risks associated with the adoption of various ICT applications in organisations. It is usually reflected in terms of various organisational strategies and policies developed and implemented across an organisation. This project aims to investigate the effectiveness and efficiency of structured approaches to ICT risk management in Thailand. The research findings would contribute to a better understanding of ICT risk management theory and practice that may lead to more effective and efficient ICT risk management planning and processes in organisations in Thailand and result in better organisational performance in today's dynamic and competitive environment.

Your participation in this project is to attend an interview conducted by me. The interview will be digitally recorded, subject to your consent, to ensure the accuracy of the transcription of the interviews. Your participation in the interview is completely voluntary, and you can withdraw from the interview at any point of time. Should you agree to participate, I can assure you that any data or information supplied will be treated in complete confidence, although the research findings may be written up in the PhD thesis or in relevant academic journals. In any event, neither individuals nor their organisations will be identified without their express permission. The data will only be retained within secure files in the School of Business IT at RMIT University for 5 years upon completion of the project (2014). Access must be given by application to the Head of School, School of Business Information Technology.

This research project is subject to the Ethics policy of RMIT. If you have any enquiries at any time about the interview or the procedures in your participation in the project, you can contact Siridech Kumsuprom by email: Siridech.kumsuprom@rmit.edu.au, or directly contact the Secretary, Portfolio Human Research Ethics Sub-committee, Business Portfolio, RMIT on telephone: (61-3) 9925 5594 or email: rdu@rmit.edu.au.

Thank you very much for your support of my research project.

Yours Faithfully,

Siridech Kumsuprom

A2. Interview question

Part I Demographic information

1. What is your position in this organisation?
2. What is your job responsibility in this organisation?

Part II The current practical ICT risk management in your organisation

3. Do you have an audit committee in your organisation?
4. In the action plan or annual plan or business plan or operational plan, does it cover IT audit and control detail?
5. What are IT audit and control details about?
6. Does it cover ICT risk management?
7. What is ICT risk management process about in that agenda?
8. In the action plan, has senior management mentioned ICT risk management?
9. What are the main concerns regarding the ICT risk management process?
10. How is ICT risk management applied in your organisation?

Part III Perception of ICT risk management in your organisation

11. Do you think each of these important? (Referred to Q 9)
12. Why do you think that each particular process is important?
13. As you mentioned before, which main process concern is the most important and why is it important?
14. Could you please rank this following process in respect to ICT risk management and give the reason why it is important for each particular process?
    - Security Policy
    - Planning and Organising
    - Organisation of Information Security
    - Asset Management
    - Access Control
    - Delivery and Support
    - Human Resource Security
    - Physical and Environment Security
    - Monitoring
    - Communication and Operation Management
    - Information System Acquisition and Development and Maintenance
    - Business Continuity Management
    - Compliance

Appendix B

SURVEY

B1. Plain language statement (English)

INVITATION TO PARTICIPATE IN A RESEARCH PROJECT

PROJECT INFORMATION STATEMENT

Project Title:

- Structured Approaches to ICT Risk Management in Thailand: An Empirical Analysis

Investigators:

- Mr Siridech Kumsuprom (Ph.D. Candidate, Business Portfolio, RMIT University, siridech.kumsuprom@rmit.edu.au, (61 3) 9925 1301)
- Professor Brian Corbitt (Senior Supervisor, Head of School, School of Business Information Technology, RMIT University, brian.corbitt@rmit.edu.au, (61 3) 9925 5808)

B2. Plain language statement (Thai)

ข้อชี้แจงทั่วไปเกี่ยวกับโครงการวิจัย

หัวข้อวิจัย การศึกษาเกี่ยวกับการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่ประสบผลสำเร็จในประเทศไทย

สถานที่วิจัย School of Business Information Technology, RMIT University, Australia

บุคลากร นายศิริเดช คำสุพรหม (นักศึกษาระดับปริญญาเอก) ผู้ดำเนินการวิจัย

Siridech Kumsuprom E-mail: e66941@rmit.edu.au

Tel: +66 080 595 1550

Tel: +61 4 1253 6763

ศาสตราจารย์ Brian Corbitt อาจารย์ที่ปรึกษา

E-mail: brian.corbitt@rmit.edu.au

Tel: +61 3 9925 5808

โครงการวิจัย เป็นไปตามที่กำหนดในหลักสูตร Doctor of Philosophy ซึ่งได้รับความเห็นชอบให้ดำเนินการวิจัยได้ และแบบสอบถามได้รับการรับรองให้ใช้ได้ จากคณะกรรมการจริยธรรมการวิจัยที่เกี่ยวข้องกับมนุษย์ (Human Research Ethics Committee—HREC) ณ สำนักงาน RMIT

B3. Letter of invitation for the survey (English)

Dear Sir/Madam,

I write to invite you to participate in my research project on the investigation of structured approaches to ICT risk management in organisations in Thailand. I am a PhD candidate at the School of Business Information Technology, RMIT University, Melbourne, Australia. My supervisor is Professor Brian Corbitt.

ICT risk management is widely used for identifying and managing the risks associated with the adoption of various ICT applications in organisations. It is usually reflected in various organisational strategies and policies developed and implemented across an organization. This project aims to investigate the success of structured approaches to ICT risk management in Thailand. The research findings would contribute to a better understanding of ICT risk management theory and practice that may lead to successful ICT risk management in organisations in Thailand and result in better organisational performance in today's dynamic and competitive environment.

Your participation in this project is to fill in an included survey. Your participation in the survey is completely voluntary, and has no perceivable risk or disadvantages as we seek only your comments and opinions regarding your understanding and practical experiences in your organisation. There is no direct benefit to you as a result of your participation. You have the rights: (a) to withdraw from the participation at any point of time; (b) to have any unprocessed data withdrawn and destroyed, provided it can be reliably identified, and provided that so doing does not increase the risk for the participant; and (c) to have any questions answered at any time. Should you agree to participate, I can assure you that any data or information supplied will be treated in complete confidence, although the research findings may be written up in the PhD thesis or in relevant academic journals. In any event, neither individuals nor their organisations will be identified without their express permission.

This research project is subject to the Ethics policy of RMIT University. If you have any enquiries at any time about the interview or the procedures in your participation of the project, you can contact Siridech Kumsuprom by email: siridech.kumsuprom@rmit.edu.au, or directly contact the Secretary, Portfolio Human Research Ethics Sub-committee, Business Portfolio, RMIT on telephone: (61-3) 9925 5594 or email: rdu@rmit.edu.au.

Thank you very much for your support of my research project.

Yours faithfully,

Siridech Kumsuprom

B4. Letter of invitation for the survey (Thai)

เรียน ท่านผู้ตอบแบบสอบถามที่เคารพ

กระผมนายศิริเดช คำสุพรหม นักศึกษาระดับปริญญาเอกของมหาวิทยาลัย RMIT ณ นครเมลเบอร์น ประเทศออสเตรเลีย ใคร่ขอเรียนเชิญท่านได้โปรดให้ความอนุเคราะห์ตอบแบบสอบถามเพื่อโครงการวิจัย หัวข้อ การศึกษาเกี่ยวกับการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่ประสบผลสำเร็จ ในประเทศไทย

ท่านได้รับการเรียนเชิญเข้าร่วมโครงการวิจัยนี้ เนื่องจากท่านมีความคุ้นเคยกับการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศในองค์กร และได้รับการเห็นชอบจากคณะกรรมการ HREC และมหาวิทยาลัย RMIT เป็นที่เรียบร้อยแล้ว

โครงการวิจัยนี้เป็นการสำรวจและค้นคว้าหาเหตุผลว่าปัจจัยอะไรที่ทำให้องค์กรบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่ประสบผลสำเร็จ ในประเทศไทย

คำชี้แจงการกระจายแบบสอบถาม

จดหมายเรียนเชิญจะถูกจัดส่งไปยังผู้บริหารระดับสูงของแต่ละฝ่ายงานที่เกี่ยวข้องกับโครงการวิจัยนี้ ขอความอนุเคราะห์รบกวนผู้บริหารฝ่ายงานโปรดส่งผ่านแบบสอบถามนี้ไปยังบุคลากรของท่านใน 2 ระดับ

ระดับ 1 ระดับผู้บริหาร แบบสอบถามจะทำการสอบถามท่านเอง 1 แบบสอบถาม และบุคคลากรที่ท่านเลือกที่อยู่ในตำแหน่งรองลงไปจากท่าน 2 แบบสอบถาม แต่ยังคงอยู่ในระดับผู้บริหาร โดยรวมทั้งสิ้น 3 แบบสอบถาม

ระดับ 2 ระดับปฏิบัติการ แบบสอบถามจะถูกส่งผ่านไปยังพนักงานในหน่วยงานของท่าน โดยทำการสุ่มเลือกบุคลากรคนใดก็ได้ในฝ่ายของท่าน รวมทั้งสิ้น 3 แบบสอบถาม

คำชี้แจงเกี่ยวกับแบบสอบถาม

ถ้าท่านตัดสินใจจะตอบแบบสอบถาม ท่านต้องใช้วิธีตอบแบบสอบถามลงในแบบสอบถามที่ได้กำหนดไว้ให้ การตอบแบบสอบถามนี้จะใช้เวลาของท่านประมาณไม่เกิน 10 นาที โดยข้อความหนึ่ง ๆ จะมีการถามอยู่สองส่วน

ส่วนที่ 1 คำถามเกี่ยวกับระดับ***การนำมาตรฐาน และแม่บทมาประยุกต์ใช้เพื่อ***การบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ

1. ไม่นำมาประยุกต์ใช้เลย < ----------> 7. นำมาประยุกต์ใช้ครบถ้วน

ส่วนที่ ๒ คำถามเกี่ยวกับระดับ***ความคิดเห็น***ของท่านที่คิดว่าบริษัทของท่านควรปฏิบัติ

1. ไม่เห็นด้วยอย่างยิ่ง <----------> 7. เห็นด้วยอย่างยิ่ง

การใช้ข้อมูลจากแบบสอบถามนี้จะไม่มีการจัดเก็บรายละเอียดเกี่ยวกับข้อมูลส่วนตัว และข้อมูลทั้งหมดในแบบสอบถามจะถูกเก็บเป็นความลับ ซึ่งมีระบบรักษาความปลอดภัยสำหรับข้อมูลภายในเครื่องคอมพิวเตอร์ส่วนบุคคลของผู้วิจัยเอง ณ มหาวิทยาลัย RMIT ผู้ดำเนินการวิจัยและอาจารย์ที่ปรึกษาเท่านั้น ที่มีสิทธิในการเข้าถึงข้อมูลดังกล่าว และผู้ดำเนินการวิจัยใช้ข้อมูลบนแบบสอบถามเพื่อการวิเคราะห์และรวบรวมเพื่อทำวิทยานิพนธ์เท่านั้น ข้อมูลที่ท่านได้ให้ไว้นั้นจะปราศจากความเสี่ยงใด ๆ

ความเห็นของท่านที่ตอบในแบบสอบถามจะเป็นประโยชน์ต่อการวิเคราะห์ในโครงการวิจัยนี้ ซึ่งจะเป็นประโยชน์อย่างยิ่งต่อการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ สำหรับองค์กรในประเทศไทยโดยตรง

การนำข้อมูลจากแบบสอบถามไปใช้ในโครงการวิจัย

- ขอให้ท่านมั่นใจได้ว่าข้อมูลในแบบสอบถามทั้งหมดจะถูกเก็บเป็นความลับอย่างเคร่งครัด ข้อมูลจะปรากฏเห็นได้เฉพาะผู้ดำเนินการวิจัย และอาจารย์ที่ปรึกษาเท่านั้น
- ข้อมูลของท่านจะถูกเปิดเผยในกรณีที่ต้องการปกป้องคุณจากความเสี่ยงที่เกี่ยวข้องเท่านั้น หรืออยู่ในคำสั่งของศาลให้เปิดเผย หรือท่านอนุญาตโดยการเขียนเป็นลายลักษณ์อักษรให้นักวิจัยท่านอื่น ๆ ได้ใช้ข้อมูล
- ข้อมูลในแบบสอบถามทั้งหมดจะถูกนำมาวิเคราะห์ร่วมกันตามหลักการทางสถิติวิเคราะห์ และผลลัพธ์ในภาพรวมที่ได้จะถูกนำไปเผยแพร่ในที่ต่าง ๆ เช่น การประชุม ลงบทความในหนังสือพิมพ์/วารสาร และวิทยานิพนธ์
- ข้อมูลทั้งหมดในแบบสอบถามของทุกท่านจะเก็บไว้ด้วยการรักษาความปลอดภัยข้อมูลข่าวสาร ณ มหาวิทยาลัย RMIT เป็นเวลา 5 ปี หลังจากการดำเนินการโครงการวิจัยแล้วเสร็จ

สิทธิของท่านต่อการตอบแบบสอบถาม

- ท่านมีสิทธิเพิกถอนที่จะไม่ร่วมตอบแบบสอบถามได้ทุกเวลา โดยปราศจากอคติ

- ท่านมีสิทธิที่จะเพิกถอนได้ทุกเวลา กรณีที่มีหลักฐานว่าท่านมีความเสี่ยงในการให้ข้อมูล
- ท่านมีสิทธิที่จะได้รับคำตอบทุกเวลาเมื่อท่านมีข้อสงสัย

หากท่านมีข้อสงสัยโปรดติดต่อ

ติดต่อโดยตรงที่ นายศิริเดช คำสุพรหม (080-595-1550) หรืออาจารย์ที่ปรึกษาตามอีเมลล์และโทรศัพท์ที่ปรากฏข้างต้น

ขอแสดงความนับถือ

นายศิริเดช คำสุพรหม

Siridech Kumsuprom

PhD Candidate (M.Inf.Sys, MBA, BAcc.)

School of Business Information Technology

Business Portfolio

RMIT University

B5. Questionnaire for ICT risk management (English)

Section A: demographics (Check only one.)

1. What is the type of your company?
   - ☐ Banking
   - ☐ Information & communication technology
   - ☐ Insurance
2. Which position level are you in?
   - ☐ The management level
   - ☐ The operational level
3. Which department you are responsible for?
   - ☐ Accounting department
   - ☐ Internal audit department
   - ☐ Information technology department
   - ☐ Information technology security department
   - ☐ Risk management department

Section B: Standard and Framework implementation

Please mark one option from the scale to what extent does your organisation implement COBIT and/or ISO/IEC 17799 in ICT risk management planning?

Statement:

The response scale is according to the following:

1. Never implemented <----------> 7. Fully implemented

Statement	**Actual Implementation**						
	Never Implemented						Fully Implemented
	1	2	3	4	5	6	7
4. Our organisation implements COBIT to deal with ICT risk management planning.							
5. Our organisation implements ISO/IEC 17799 to deal with ICT risk management planning.							

6. What other standards and/or frameworks does your organisation implement to deal with ICT risk management planning? Please specify……..……

Section C: Successful ICT risk management in the organisation

Please ☒ mark one option from the scale to show to what extent you agree or disagree with each statement when you are dealing with ICT risk management in your organisation.

Statement: For the statements below, there are two types of question on each item to be asked about:

*A: To what extent **do you think** your organisation should implement COBIT and ISO/IEC 17799 in ICT risk management planning?* Level of agreement with the statements is represented by a scale of 1-7 as per the following:

1. Strongly disagree <----------> 7. Strongly agree

Policy

How does the organisational policy affect the corporate level plan (the corporate plan) and the operational level plan (the action plan) in respect to successful ICT risk management?

Statement	**Attitude**						
	Strongly Disagree						Strongly Agree
	1	2	3	4	5	6	7
7. The organisation defines technological direction in the organisational policy.							
8. The organisation defines security direction in the organisational policy.							
9. The organisation establishes risk context to define the definition of ICT risks.							
10. The organisation has a business continuity plan to face the uncertain circumstance regarding the loss of information asset.							

Strategy direction

How does the organisational strategy affect the corporate level plan (the corporate plan) and the operational level plan (the action plan) in respect to successful ICT risk management?

Statement	**Attitude**						
	Strongly Disagree						Strongly Agree
	1	2	3	4	5	6	7
11. The organisational strategies in ICT risk management are generated by management.							
12. The organisational strategies in ICT risk management are generated by the operational level.							

Human resource management and planning

How do human resource management and planning affect the corporate plan (corporate level) and the action plan (operational level) in respect to successful ICT risk management?

Statement	Attitude						
	Strongly Disagree						Strongly Agree
	1	2	3	4	5	6	7
13. The organisation defines employees' roles regarding information governance policy.							
14. The organisation defines employees' responsibilities regarding information governance policy.							
15. The organisation defines employees' roles regarding information security governance policy.							
16. The organisation defines employees' responsibilities regarding information security governance policy.							
17. The organisation declares terms and conditions of employment regarding confidentiality of information.							
18. The organisation informs employees not to disclose the organisation's important information.							
19. The organisation provides a training program to improve staff's IT awareness.							
20. The organisation provides a training program to improve staff's IT security awareness.							
21. The organisation changes access rights of employees upon change of employment.							
22. The organisation removes access rights of employees upon termination of employment.							

Security

How does information technology security affect the corporate plan (corporate level) and the action plan (operational level) in respect to successful ICT risk management?

Statement	Attitude						
	Strongly Disagree						Strongly Agree
	1	2	3	4	5	6	7
23. The organisation correctly configures its operating systems (e.g. Windows, Linux and Unix).							
24. The organisation correctly configures its networking operating systems (e.g. NetWare and Cisco).							
25. The organisation correctly configures its business software (e.g. SAP and business solution).							
26. The organisation correctly configures its hardware (e.g. AS 400, hubs, switches, routers).							

27. The organisation documents access control following business requirements for system access.							
28. The organisation allows only authorised persons to have access to network services.							
29. The organisation strictly limits access to computer use by user allocation.							
30. The organisation strictly limits access to computers by using a password management system.							
31. The organisation monitors log files to prevent unauthorised access.							
32. The organisation monitors computer use to prevent computer abuse.							
33. The organisation monitors computer use in order to prevent any type of damage to information asset.							
34. The organisation validates input data from applications systems for its correctness before putting data into the input process.							
35. The organisation validates input data from applications systems for its appropriateness before putting data into the input process.							
36. The organisation has validation check applications to detect any corruption of information through processing errors.							
37. The organisation has validation check applications to detect any corruption of information through deliberate acts.							
38. The organisation validates output data from applications systems for its correctness before being distributed.							
39. The organisation validates output data from applications systems for its appropriateness before being distributed.							
40. The organisation controls application system files in a secure manner (control of operational software).							
41. The organisation controls application system files in a secure manner (protection of system test).							
42. The organisation regularly checks IT facilities for compliance with security implementation standards.							
43. All departments within the organisation have regular review plans to ensure compliance with security policy and standards.							
44. The organisation identifies compliance with legal requirements (e.g. Thailand's *Computer Crime Act*).							
45. The organisation monitors data protection and privacy.							
46. The organisation prevents data protection and privacy.							
47. The organisation prevents unauthorised physical access, damage and interference to the organisation's premises and information systems.							

Technology

How does technology affect the corporate plan (corporate level) and the action plan (operational level) in respect to successful ICT risk management?

Statement	Attitude						
	Strongly Disagree						Strongly Agree
	1	2	3	4	5	6	7
48. The organisation provides a sufficient networking connection to employees.							
49. The organisation provides sufficient personal access to computers for employees.							
50. The organisation manages several types of operating software in order to generate data and information in the same file pattern.							
51. The organisation provides all applications with legal of use.							

Corporate level

How does the corporate level affect successful ICT risk management?

Statement	Attitude						
	Strongly Disagree						Strongly Agree
	1	2	3	4	5	6	7
52. The organisation has established IT control and audit in the corporate plan regarding the organisation objectives.							
53. The organisation provides an overview of IT applications and IT security in the IT plan.							
54. The organisation provides an overview of ICT risk management methodology.							

Operational level

How does the operational level affect successful ICT risk management?

Statement	Attitude						
	Strongly Disagree						Strongly Agree
	1	2	3	4	5	6	7
55. The organisation has established information security control and audit in the action plan for the specific department.							
56. The organisation provides information security in security direction.							
57. The organisation provides IT risk project management methodology for a specific project.							

Successful ICT risk management

How does successful ICT risk management affect ICT risks?

Statement	Attitude						
	Strongly Disagree						Strongly Agree
	1	2	3	4	5	6	7
58. Successful ICT risk management helps the organisation mitigate ICT risks to risk appetites (acceptable level).							
59. Successful ICT risk management helps the organisation prevent ICT risks appropriately.							
60. Successful ICT risk management helps the organisation avoid ICT risks appropriately.							

B6. Questionnaire for ICT risk management (Thai)

แบบสอบถาม การบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ

หมวด ๑ ลักษณะทั่วไปของผู้ให้สัมภาษณ์ (โปรดกากบาท X เพียงคำตอบเดียวเท่านั้น)

๑. องค์กรที่ท่านทำงานอยู่ในปัจจุบันดำเนินธุรกิจประเภทใด

- ☐ ธนาคาร
- ☐ เทคโนโลยีสารสนเทศ และการสื่อสาร
- ☐ การประกันภัย

๒. ท่านมีตำแหน่งหน้าที่ในองค์กรอยู่ในระดับใด

- ☐ ระดับผู้บริหาร
- ☐ ระดับปฏิบัติการ

๓. ท่านมีความรับผิดชอบต่อองค์กรในแผนกใด

- ☐ ฝ่ายบัญชีและการเงิน
- ☐ ฝ่ายตรวจสอบภายใน
- ☐ ฝ่ายเทคโนโลยีสารสนเทศ
- ☐ ฝ่ายบริหารความปลอดภัยเทคโนโลยีสารสนเทศ
- ☐ ฝ่ายบริหารความเสี่ยง

หมวด ๒ มาตรฐาน (Standard) และแม่บท (Framework) เกี่ยวกับการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ

โปรดกากบาท (X) ลงในระดับการนำมาตรฐาน และแม่บทมาช่วยการวางแผนการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ

คำชี้แจง ระดับการนำมาตรฐาน และแม่บทมาช่วยการวางแผนการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ

๑. ไม่นำมาใช้เลย < ----------> ๗. นำมาใช้ครบถ้วน

รายละเอียด	การนำมาประยุกต์ใช้ในองค์กร						
	ไม่นำมาใช้เลย						นำมาใช้ครบถ้วน
	๑	๒	๓	๔	๕	๖	๗
๔. บริษัทนำ แม่บทการกำกับดูแลกิจการด้านเทคโนโลยีสารสนเทศ COBIT (IT Governance) มาช่วยในการวางแผนการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ							
๕. บริษัทนำ มาตรฐานกำกับดูแลกิจการด้านความปลอดภัยเทคโนโลยีสารสนเทศ ISO/IEC 17799 / BS 7799 (Information Security Governance) มาช่วยในการวางแผนการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ							

๖. บริษัทนำมาตรฐาน และแม่บทอื่น ๆ มาช่วยการวางแผนการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ อะไรบ้าง โปรดระบุ.....

.....

หมวด ๓ การบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่ประสบผลสำเร็จในองค์กร

โปรดกากบาท (X) ลงในระดับการนำมาประยุกต์ใช้ และระดับความคิดเห็นของท่านเกี่ยวกับการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่ประสบผลสำเร็จในองค์กร เมื่อท่านกำลังบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศภายในองค์กร ตามข้อความข้างล่างนี้ และโปรดอ่านคำชี้แจงให้ละเอียด

คำชี้แจง สำหรับข้อความข้างล่าง มีคำถามอยู่ ๒ ลักษณะ

ก. คำถามเกี่ยวกับระดับ***ความคิดเห็น***ของท่านที่คิดว่าบริษัทของท่านควรปฏิบัติ

๑. *ไม่เห็นด้วยอย่างยิ่ง* <----------><u>๗</u>. *เห็นด้วยอย่างยิ่ง*

นโยบาย (Policy)

ระดับการนำมาประยุกต์ใช้ และระดับความคิดเห็นทางด้านนโยบายขององค์กรมีความสัมพันธ์ต่อ การกำหนดแผนงานประจำปีขององค์กร (The corporate plan/Corporate Level) และ แผนงานปฏิบัติการขององค์กร (The action plan/ Operational Level) ที่เกี่ยวข้องกับการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศเป็นอย่างไร

รายละเอียด	**ระดับความคิดเห็น**						
	ไม่เห็นด้วยอย่างยิ่ง						เห็นด้วยอย่างยิ่ง
	๑	๒	๓	๔	๕	๖	๗
๗. องค์กรกำหนดแนวทางด้านเทคโนโลยีสารสนเทศภายในนโยบายหลักขององค์กร							
๘. องค์กรกำหนดแนวทางด้านความปลอดภัยทางเทคโนโลยีสารสนเทศ ภายในนโยบายหลักขององค์กร							
๙. องค์กรกำหนดการบริหารความเสี่ยง โดยอธิบายความหมายของความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศขององค์กรไว้ชัดเจนโดยละเอียด (Risk Statement)							
๑๐. องค์กรกำหนดแผนการทำงานอย่างต่อเนื่อง (Business continuity plan) เมื่อองค์กรเผชิญปัญหาที่เกี่ยวข้องกับสถานการณ์ที่ไม่แน่นอน ในเรื่องการสูญเสียสารสนเทศ (Information) ขององค์กร							

แนวทางกลยุทธ์ขององค์กร (Strategy direction)

ระดับการนำมาประยุกต์ใช้ และระดับความคิดเห็นทางด้านแนวทางกลยุทธ์ขององค์กรมีความสัมพันธ์ต่อ การกำหนดแผนงานประจำปีขององค์กร (The corporate plan/Corporate Level) และ แผนงานปฏิบัติการขององค์กร (The action plan/ Operational Level) ที่เกี่ยวข้องกับการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศเป็นอย่างไร

รายละเอียด	ระดับความคิดเห็น						
	ไม่เห็นด้วยอย่างยิ่ง						เห็นด้วยอย่างยิ่ง
	๑	๒	๓	๔	๕	๖	๗
๑๑. ผู้บริหารระดับสูงกำหนดกลยุทธ์ขององค์กรที่เกี่ยวข้องกับการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ							
๑๒. ผู้บริหารระดับปฏิบัติการกำหนดกลยุทธ์ขององค์กรที่เกี่ยวข้องกับการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ							

การจัดการทรัพยากรมนุษย์ และการวางแผนทรัพยากรมนุษย์ (Human resource management and planning)

ระดับการนำมาประยุกต์ใช้ และระดับความคิดเห็นทางด้านการจัดการทรัพยากรมนุษย์ และการวางแผนทรัพยากรมนุษย์ขององค์กรมีความสัมพันธ์ต่อ การกำหนดแผนงานประจำปีขององค์กร (The corporate plan/Corporate Level) และ แผนงานปฏิบัติการขององค์กร (The action plan/ Operational Level) ที่เกี่ยวข้องกับการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศเป็นอย่างไร

รายละเอียด	ระดับความคิดเห็น						
	ไม่เห็นด้วยอย่างยิ่ง						เห็นด้วยอย่างยิ่ง
	๑	๒	๓	๔	๕	๖	๗
๑๓. พนักงานเข้าใจบทบาทของตนเองที่เกี่ยวกับนโยบายเทคโนโลยีธรรมาภิบาล (Information governance policy)							
๑๔. พนักงานเข้าใจหน้าที่ความรับผิดชอบของตนเองที่เกี่ยวกับนโยบายเทคโนโลยีธรรมาภิบาล (Information governance policy)							
๑๕. พนักงานเข้าใจบทบาทของตนเองที่เกี่ยวกับนโยบายความปลอดภัยของข้อมูลธรรมาภิบาล (Information Security policy)							
๑๖. พนักงานเข้าใจหน้าที่ความรับผิดชอบของตนเองที่เกี่ยวกับนโยบายความปลอดภัยของข้อมูลธรรมาภิบาล (Information Security policy)							
๑๗. พนักงานเข้าใจเงื่อนไขในสัญญาในการจ้างงานที่เกี่ยวข้องกับการเก็บความลับข้อมูลที่สำคัญขององค์กร							

๑๘. พนักงานไม่เปิดเผยข้อมูลที่สำคัญขององค์กรต่อบุคคลภายนอก							
๑๙. การฝึกอบรมและการเรียนรู้ในองค์กรช่วยให้พนักงานเพิ่มความระมัดระวังในการปฏิบัติงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (Staff's IT awareness)							
๒๐. การฝึกอบรมและการเรียนรู้ในองค์กรช่วยให้พนักงานเพิ่มความระมัดระวังในความปลอดภัยทางด้านเทคโนโลยีสารสนเทศ (Staff's security awareness)							
๒๑. องค์กรยกเลิกสิทธิการเข้าถึงข้อมูลของพนักงาน จากแผนกเดิมเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน หรือย้ายงาน และให้ได้รับสิทธิในแผนกใหม่							
๒๒. องค์กรยกเลิกสิทธิ์ในการเข้าถึงข้อมูลของพนักงานเมื่อลาออก หรือสิ้นสุดการทำงาน							

ความปลอดภัยทางด้านเทคโนโลยีสารสนเทศ (Information Technology Security)

ระดับการนำมาประยุกต์ใช้ และระดับความคิดเห็นทางด้านความปลอดภัยทางด้านเทคโนโลยีสารสนเทศขององค์กรมีความสัมพันธ์ต่อ การกำหนดแผนงานประจำปีขององค์กร (The corporate plan/Corporate Level) และ แผนงานปฏิบัติการขององค์กร (The action plan/ Operational Level) ที่เกี่ยวข้องกับการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศเป็นอย่างไร

รายละเอียด	**ระดับความคิดเห็น**						
	ไม่เห็นด้วยอย่างยิ่ง						เห็นด้วยอย่างยิ่ง
	๑	๒	๓	๔	๕	๖	๗
๒๓. ซอฟแวร์ในระบบปฏิบัติการ (Operation system) เช่น Windows server, Linux และ Unix มีการกำหนดค่าคุณสมบัติ (Configuration) ได้ถูกต้อง							
๒๔. ซอฟแวร์ในระบบเครือข่าย (Networking operating systems) เช่น Netware และ Cisco มีการกำหนดค่าคุณสมบัติ (Configuration) ได้ถูกต้อง							
๒๕. ซอฟแวร์ทางธุรกิจ (Business software) เช่น SAP และ Business solution มีการกำหนดค่าคุณสมบัติ (Configuration) ได้ถูกต้อง							
๒๖. อุปกรณ์ทางเทคโนโลยีสารสนเทศ (Hardware) เช่น AS/400, Hubs, Switches และ Routers มีการกำหนดค่าคุณสมบัติ (Configuration) ได้ถูกต้อง							
๒๗. การควบคุมเกี่ยวกับการเข้าถึงข้อมูลมีการกำหนดเป็นลายลักษณ์อักษรเพื่อให้สอดคล้องกับความต้องการทางธุรกิจที่เกี่ยวข้องกับระบบการเข้าถึงข้อมูล							
๒๘. องค์กรควบคุมการเข้าถึงระบบเครือข่าย (Network) โดยอนุญาตให้เฉพาะผู้ที่เกี่ยวข้องกับการทำงานในระบบเครือข่ายเท่านั้น							
๒๙. องค์กรควบคุมการใช้คอมพิวเตอร์ส่วนบุคคล (Personal Computer) โดยระบุผู้ใช้ของเครื่องคอมพิวเตอร์							
๓๐. องค์กรควบคุมการใช้คอมพิวเตอร์ส่วนบุคคล (Personal Computer) โดย							

การกำหนดรหัสผ่านของเครื่องคอมพิวเตอร์							
๓๑. องค์กรตรวจสอบ log file ของการเข้าระบบ เพื่อดูการเข้ามาใช้ระบบที่ไม่ถูกต้อง							
๓๒. องค์กรตรวจสอบ การใช้คอมพิวเตอร์ส่วนบุคคลของพนักงาน เพื่อป้องกันการใช้คอมพิวเตอร์ผิดวัตถุประสงค์ และป้องกันความเสียหายต่าง ๆ							
๓๓. องค์กรตรวจสอบ การใช้คอมพิวเตอร์ส่วนบุคคลของพนักงาน เพื่อป้องกันความเสียหายต่าง ๆ							
๓๔. องค์กรมีการตรวจสอบข้อมูลอย่างถูกต้อง ก่อนที่จะทำการนำเข้าข้อมูล (Input data)							
๓๕. องค์กรมีการตรวจสอบข้อมูลอย่างเหมาะสม ก่อนที่จะทำการนำเข้าข้อมูล (Input data)							
๓๖.องค์กรมีโปรแกรมที่ใช้ในการตรวจสอบระหว่างการประมวลผลข้อมูลเพื่อตรวจจับความผิดพลาดของข้อมูล							
๓๗. องค์กรมีโปรแกรมที่ใช้ในการตรวจสอบระหว่างการประมวลผลข้อมูลเพื่อตรวจจับวิธีปฏิบัติการประมวลผลข้อมูลที่ผิดพลาด							
๓๘. องค์กรมีการตรวจสอบข้อมูลผลลัพธ์ด้วยความถูกต้องก่อนที่จะนำเสนอ (Output data)							
๓๙. องค์กรมีการตรวจสอบข้อมูลผลลัพธ์ด้วยความเหมาะสมก่อนที่จะนำเสนอ (Output data)							
๔๐. องค์กรมีการควบคุมโปรแกรมที่ใช้งานการปฏิบัติงาน							
๔๑. องค์กรมีการควบคุมระบบทดสอบการป้องกันทางด้านเทคโนโลยีสารสนเทศภายในองค์กร							
๔๒. องค์กรมีการตรวจสอบความสามารถของเทคโนโลยีสารสนเทศ (IT Facilities) เป็นประจำเพื่อให้สอดคล้องกับการประยุกต์ใช้มาตรฐานความปลอดภัยทางเทคโนโลยีสารสนเทศ							
๔๓. ทุกแผนกในองค์กรมีแผนงานตรวจสอบ (Audit plan) อยู่เป็นประจำ เพื่อมั่นใจได้ว่าทุกขั้นตอนการปฏิบัติงานได้เป็นไปตามนโยบายความปลอดภัยของเทคโนโลยีสารสนเทศ							
๔๔. องค์กรระบุระเบียบปฏิบัติทางด้านความปลอดภัยเทคโนโลยีสารสนเทศให้สอดคล้องกับความต้องการของกฎหมาย (พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐)							
๔๕. องค์กรมีการตรวจสอบความปลอดภัยของข้อมูลและข้อมูลส่วนบุคคล							
๔๖. องค์กรมีการป้องกันความปลอดภัยของข้อมูลและข้อมูลส่วนบุคคล							
๔๗. องค์กรป้องกันการเข้า-ออกของบุคคลที่ไม่ได้รับอนุญาตซึ่งอาจก่อให้เกิดความเสียหายต่อทรัพย์สิน และสารสนเทศขององค์กร							

เทคโนโลยีสารสนเทศ (Information Technology)

ระดับการนำมาประยุกต์ใช้ และระดับความคิดเห็นทางด้านเทคโนโลยีสารสนเทศขององค์กรมีความสัมพันธ์ต่อ การกำหนดแผนงานประจำปีขององค์กร (The corporate plan/Corporate Level) และ แผนงานปฏิบัติการขององค์กร (The action plan/ Operational Level) ที่เกี่ยวข้องกับการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศเป็นอย่างไร

รายละเอียด	ระดับความคิดเห็น						
	ไม่เห็นด้วยอย่างยิ่ง						เห็นด้วยอย่างยิ่ง
	๑	๒	๓	๔	๕	๖	๗
๔๘. องค์กรมีการตระเตรียมจุดเชื่อมต่อเครือข่าย (Hub) เพียงพอสำหรับพนักงาน							
๔๙. องค์กรมีการตระเตรียมเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) เพียงพอสำหรับพนักงาน							
๕๐. องค์กรจัดการข้อมูล และสารสนเทศ จากโปรแกรมปฏิบัติงานต่าง ๆ ให้อยู่ในลักษณะที่นำมาใช้ร่วมกันได้							
๕๑. องค์กรตระเตรียมโปรแกรมที่ใช้ในการปฏิบัติงานทุกโปรแกรมภายใต้ลิขสิทธิ์นั้น ๆ							

แผนงานประจำปี (Corporate level plan)

ระดับการนำมาประยุกต์ใช้ และระดับความคิดเห็นทางด้านแผนงานประจำปีในระดับ Corporate มีความสัมพันธ์ต่อ การบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่ประสบผลสำเร็จในองค์กรเป็นอย่างไร

รายละเอียด	ระดับความคิดเห็น						
	ไม่เห็นด้วยอย่างยิ่ง						เห็นด้วยอย่างยิ่ง
	๑	๒	๓	๔	๕	๖	๗
๕๒. องค์กรกำหนดหัวข้อการตรวจสอบและควบคุมทางด้านเทคโนโลยีสารสนเทศในแผนงานประจำปีภายใต้วัตถุประสงค์ขององค์กร							
๕๓. องค์กรวางแผนภาพรวมของ IT application และ IT security หรือ General IT และ IT security ในแผนงานประจำปี							
๕๔. องค์กรกำหนดขั้นตอนกระบวนการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ (ICT risk management methodology)							

แผนงานปฏิบัติการ (Operational level plan)

ระดับการนำมาประยุกต์ใช้ และระดับความคิดเห็นทางด้านแผนงานปฏิบัติการในระดับ Operation มีความสัมพันธ์ต่อ การบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่ประสบผลสำเร็จในองค์กรเป็นอย่างไร

รายละเอียด	ระดับความคิดเห็น						
	ไม่เห็นด้วยอย่างยิ่ง						เห็นด้วยอย่างยิ่ง
	๑	๒	๓	๔	๕	๖	๗
๕๕. องค์กรกำหนดหัวข้อการตรวจสอบและควบคุมทางด้าน Technical security ชัดเจนในแผนงานปฏิบัติการ สำหรับแต่ละแผนก							
๕๖. องค์กรกำหนดรายละเอียดของการควบคุมทางด้าน Technical security ชัดเจนในแผนงานปฏิบัติการสำหรับแต่ละแผนก							
๕๗. องค์กรกำหนดขั้นตอนกระบวนการบริหารความเสี่ยงทางเทคโนโลยีสารสนเทศสำหรับเฉพาะโครงการ (ICT risk project management methodology)							

การบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่ประสบผลสำเร็จ (Successful ICT risk management)

ระดับความคิดเห็นทางด้านการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ มีความสัมพันธ์ต่อความเสี่ยงทางด้านเทคโนโลยีสารสนเทศอย่างไร

รายละเอียด	ก. ระดับความคิดเห็น						
	ไม่เห็นด้วยอย่างยิ่ง						เห็นด้วยอย่างยิ่ง
	1	2	3	4	5	6	7
๕๘. ท่านคิดว่าการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่ประสบผลสำเร็จช่วยให้องค์กรลดความเสี่ยงทางด้านเทคโนโลยีสารสนเทศในระดับที่ยอมรับได้ (Risk appetite)							
๕๙. ท่านคิดว่าการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่ประสบผลสำเร็จช่วยให้องค์กรป้องกันความเสี่ยงทางด้านเทคโนโลยีสารสนเทศได้ด้วยความเหมาะสม							
๖๐. ท่านคิดว่าการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่ประสบผลสำเร็จช่วยให้องค์กรหลีกเลี่ยงความเสี่ยงทางด้านเทคโนโลยีสารสนเทศได้ด้วยความเหมาะสม							

Appendix C

SAMPLE COVARIANCE MATRIX

C1. Sample covariances matrix (Successful ICT risk management)

	it4	policy3	esp5	esp4	esp3	esp2	sictrm3	sictrm2	sictrm1	policy1	policy2	it3	it1
ict4	1.162												
policy3	.701	1.862											
esp5	.829	1.001	1.499										
esp4	.807	1.023	1.157	1.268									
esp3	.788	.944	1.065	1.040	1.077								
esp2	.707	.892	1.000	.925	.903	1.015							
sictrm3	.515	.439	.568	.567	.520	.498	.996						
sictrm2	.506	.537	.666	.646	.584	.580	.814	.942					
sictrm1	.585	.592	.721	.701	.631	.639	.881	.907	1.169				
policy1	.583	1.198	.851	.829	.742	.748	.420	.476	.584	1.427			
policy2	.655	1.271	.927	.897	.797	.787	.431	.502	.583	1.192	1.427		
ict3	.954	.704	.830	.830	.774	.688	.552	.572	.642	.601	.654	1.161	
ict1	.892	.709	.824	.836	.772	.737	.639	.671	.768	.660	.657	.963	1.374